Verification of Translation

I, Robin Holding, having an office at 948 15th Street, #4, Santa Monica, CA 90403-3134, hereby state that I am well acquainted with both the English and French languages and that to the best of my knowledge and ability, the appended document is a true and faithful translation of

Int'l. Patent Application No. PCT/FR00/03230

In the name of BULL S.A., Inventors: CUNCHON ET AL.

Filed on 21 November 2000

I further declare that the above statement is true; and further, that this statement is made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent resulting therefrom.

July 19, 2000
Date

Robin Holding
Robin Holding

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
31 mai 2001 (31.05.2001)

PCT

(10) Numéro de publication internationale
WO 01/39466 A1

(51) Classification internationale des brevets[7]: H04L 29/06, G06F 9/46

(21) Numéro de la demande internationale:
PCT/FR00/03230

(22) Date de dépôt international:
21 novembre 2000 (21.11.2000)

(25) Langue de dépôt: français

(26) Langue de publication: français

(30) Données relatives à la priorité:
99/14755 23 novembre 1999 (23.11.1999) FR

(71) Déposant *(pour tous les États désignés sauf US)*: **BULL S.A.** [FR/FR]; 68, route de Versailles, F-78430 Louveciennes (FR).

(72) Inventeurs; et

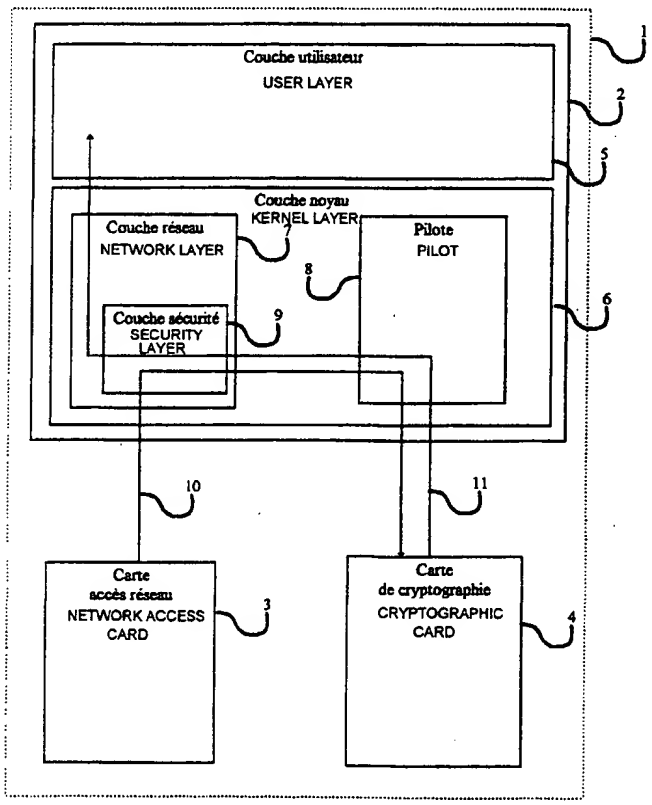
(75) Inventeurs/Déposants *(pour US seulement)*: **CUNCHON, François** [FR/FR]; 5, rue Claude Nicolas Ledoux, F-78114 Magny Les Hameaux (FR). **MARTIN, René** [FR/FR]; 32, rue Gometz, F-91440 Bures sur Yvette (FR). **TRAN MINH, Lap** [FR/FR]; 18, rue Paul Eluard, F-95360 Montmagny (FR).

(74) Mandataire: **COLOMBE, Michel**; Bull S.A., 68, route de Versailles, F-78434 Louveciennes Cedex (FR).

[Suite sur la page suivante]

(54) Title: COMPUTER DEVICE FOR MAKING SECURE MESSAGES AT A NETWORK LAYER

(54) Titre: DISPOSITIF INFORMATIQUE POUR SECURISER DES MESSAGES AU NIVEAU D'UNE COUCHE RESEAU



(57) Abstract: The invention concerns a computer device (1) comprising a storage unit and a network security layer (9) for applying a security processing when a message (M1) is presented in the storage unit (2). The invention is characterised in that the presentation of the message (M1) shifts the network security layer (9) from an initial state (12) to a first state (25) which produces a backup of the execution context (CE) in a zone (52) of the storage unit (2); the production of the executing context backup (CE) shifts the network security layer from the first state (25) to a second state (33) which calls a first function (F9) for processing the message (M1), carrying as parameters of said first function (F9), at least an address (@F13) of second function (F13) and a pointer PZS (M1) on the zone (52) of the storage unit (2); an acknowledgement of the first function (F9) before processing the message (M1), immediately shifts back the network security layer into the initial state (12); a connection on the address (@F13) of second function, shifts the network security layer (9) from the initial state (12) to a third state (56) which restores the executing context (CE) before shifting back the network security layer (9) into the initial state.

WO 01/39466 A1

[Suite sur la page suivante]

(81) **État désigné** *(national)*: US.

(84) **États désignés** *(régional)*: brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

Publiée:

— *Avec rapport de recherche internationale.*

— *Avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues.*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(57) Abrégé: Le dispositif informatique (1) comprenant une mémoire (2) et une couche de sécurité réseau (9) pour appliquer un traitement de sécurisation sur présentation d'un message (M1) dans la mémoire (2), est caractérisé en ce que: la présentation du message (M1) fait passer la couche de sécurité réseau (9) d'un état initial (12) à un premier état (25) qui réalise une sauvegarde de contexte d'exécution (CE) dans une zone (52) de la mémoire (2); la réalisation de la sauvegarde du contexte d'éxécution (CE), fait passer la couche de sécurité réseau du premier état (25) à un deuxième état (33) qui appelle une première fonction (F9) de traitement du message (M1), en passant comme paramètres de ladite première fonction (F9), au moins une adresse (@F13) de deuxième fonction (F13) et un pointeur PZS (M1) sur la zone (52) de la mémoire (2); un acquittement de la première fonction (F9) avant traitement du message (M1), fait immédiatement repasser la couche de sécurité réseau dans l'état initial (12); un branchement sur l'adresse (@F13) de deuxième fonction, fait passer la couche de sécurité réseau (9) de l'état intial (12) à un troisième état (56) qui réalise une restitution du contexte d'exécution (CE) avant de faire repasser la couche de sécurité réseau (9) dans l'état intitial.

Dispositif informatique pour sécuriser des messages au niveau d'une couche réseau.

Le domaine de l'invention est celui des réseaux informatiques et plus particulièrement celui de la sécurisation d'acheminement de messages sur ces réseaux.

Un réseau public tel que le réseau Internet, permet d'interconnecter de nombreux réseaux privés reliés par des points d'accès et des routeurs qui acheminent les messages. La facilité d'accès à un tel réseau est un avantage pour le libre parcours des idées et de nombreuses connaissances, c'est aussi un inconvénient pour la confidentialité de certaines informations. C'est pourquoi il convient de sécuriser certains messages de façon à ce que seul le destinataire puisse les comprendre, soit assuré de leurs provenances et ou de leur intégrité.

Un traitement de sécurisation de messages est envisageable dans différentes couches de communication d'un dispositif informatique. Par exemple, dans une couche utilisateur, une application telle que http, ftp ou mail, peut se charger d'effectuer des traitements de cryptage et décryptage, de signature et d'authentification. Généralement, le message n'est disponible que dans la couche utilisateur de l'émetteur initial et du récepteur final.

Selon l'état de la technique, on peut prévoir de faire le traitement de sécurisation dans une couche réseau où une couche de sécurité réseau telle que Ipsec prend en charge le traitement de sécurisation au niveau même du routage des messages. Ceci permet de créer des réseaux privés virtuels qui empruntent les ressources du réseau public au moyen d'un effet tunnel connu. La couche réseau est généralement considérée comme une ressource de communication d'un dispositif informatique. La mise en œuvre de la couche de sécurité réseau qui résulte de cette considération, dans la couche noyau d'un système d'exploitation du dispositif informatique, décharge alors la couche utilisateur des traitements de sécurisation.

Cependant, certains traitements de sécurisation sont longs car ils appliquent de nombreux calculs sur le contenu d'un message à sécuriser. Une attente du système d'exploitation sur un retour de fonction qui donne le résultat de traitement présente l'inconvénient de bloquer le dispositif informatique.

L'objet de l'invention est un dispositif informatique comprenant une mémoire et une couche de sécurité réseau pour appliquer un traitement de sécurisation sur présentation d'un message dans la mémoire. Pour pallier l'inconvénient précédemment cité, le dispositif informatique est caractérisé en ce que:

- la présentation du message fait passer la couche de sécurité réseau d'un état initial à un premier état qui réalise une sauvegarde de contexte d'exécution dans une zone de la mémoire;
- la réalisation de la sauvegarde du contexte d'exécution, fait passer la couche de sécurité réseau du premier état à un deuxième état qui appelle une première fonction de traitement du message, en passant comme paramètres de ladite première fonction, au moins une adresse de deuxième fonction et un pointeur sur la zone de la mémoire;
- un acquittement de la première fonction avant traitement du message, fait immédiatement repasser la couche de sécurité réseau dans l'état initial;
- un branchement sur l'adresse de deuxième fonction après traitement du message, fait passer la couche de sécurité réseau de l'état initial à un troisième état qui réalise une restitution du contexte d'exécution avant de faire repasser la couche de sécurité réseau dans l'état initial.

Dans l'état initial, la couche de sécurité réseau n'utilise aucune ressource du dispositif informatique. Le retour de la couche de sécurité réseau dans son état initial sans attendre une fin de traitement du message évite de bloquer le dispositif informatique. La sauvegarde du contexte d'exécution permet de replacer en fin de traitement de message, la couche de sécurité réseau dans le contexte où elle était avant que le traitement commence. Ainsi, le traitement de sécurisation du message est effectué de façon asynchrone.

Une description de mise en œuvre particulière de l'invention, suit en référence aux figures où:

- la figure 1 représente une architecture de réseau sécurisé;
- la figure 2 représente un dispositif informatique pour traiter des messages;
- la figure 3 représente les étapes essentielles d'une couche de traitement de sécurité sous forme de machine à nombre fini d'états de l'état de la technique;
- les figures 4 et 5 représentent les étapes essentielles d'une couche de traitement de sécurité sous forme de machine à nombre fini d'états conforme à l'invention;

- la figure 6 représente les étapes essentielles d'un pilote de carte de traitement matériel sous forme de machine à nombre fini d'états pour mettre en œuvre la machine selon les figures 3 et 4.
- la figure 7 représente une architecture de zones de sauvegardes en mémoire;
- la figure 8 présente une première étape d'un procédé de réalisation de code d'une couche de sécurité réseau;
- la figure 9 présente une deuxième étape du procédé de réalisation de code d'une couche de sécurité réseau;
- la figure 10 présente un procédé de production de messages sécurisés.

En référence à la figure 1, un dispositif informatique 67 est physiquement relié à un premier réseau privé 69 et un dispositif informatique 68 est physiquement relié à un deuxième réseau privé 70. Des messages peuvent circuler en toute confidentialité sur chacun des réseaux privés 69 et 70 dans la mesure où aucune intrusion ne peut être effectuée de l'extérieur sur ces réseaux. Cependant, si le dispositif 67 envoie un message au dispositif 68 en utilisant des services d'un réseau public 71, la confidentialité n'est pas assurée sans prendre de précautions particulières. Le réseau public 71 est par exemple le réseau connu sous le nom d'Internet, souvent représenté sous forme d'un nuage dans la littérature. Le réseau public 71 regroupe plusieurs réseaux 72, 73, interconnectés au moyens de dispositifs informatiques tels qu'un dispositif informatique 65 non contrôlé par les dispositifs 67, 68.

Le réseau privé 69 est relié au réseau public 71 par un dispositif informatique 66 et le réseau privé 70 est relié au réseau public 71 par un dispositif informatique 1. Les dispositifs informatiques 1 et 66 sont appelés passerelles dans la suite de la description. Chaque dispositif informatique 1, 65, 66, 67, 68 comprend traditionnellement une couche réseau utilisant un protocole de communication tel que le protocole connu IP, surmonté d'une couche transport utilisant un protocole tel que le protocole connu TCP, UDP ou autre, surmonté à son tour d'une couche applicative telle que http, ftp ou autre qui émettent et reçoivent des messages. Si un message traverse les couches TCP puis IP dans le dispositif 67 et traverse les couches IP puis TCP dans le dispositif 68, l'acheminement du message à travers le réseau public 71 reste normalement dans les couches IP des dispositifs 66, 65, 1.

Cependant, le dispositif 65 peut favoriser une intrusion étrangère sur les réseaux 72, 73 avec un danger de capter le message pour le lire, le modifier, voire de générer un message en se faisant passer pour le dispositif 67. Une solution consiste à crypter et/ou signer le message dans la couche IP de la passerelle 66, à sa sortie sur le réseau d'interconnexion 72, puis de décrypter le message dans la couche IP de la passerelle 1, à son entrée du réseau d'interconnexion 73. Une solution connue sous le nom d'Ipsec, permet ainsi de créer un tunnel 74 qui traverse le réseau public 71, de façon à créer un réseau privé virtuel utilisables par les dispositifs 67 et 68.

En référence à la figure 2, un dispositif informatique 1 comprend une mémoire 2, une ou plusieurs cartes d'accès réseau 3 et une ou plusieurs cartes de cryptographie 4. La carte d'accès réseau 3 est destinée à être raccordée sur une ou plusieurs liaisons physiques, non représentées. La mémoire 2, de type connu tel que les mémoires à accès aléatoire RAM, est destinée à contenir des données et des programmes de traitement du dispositif informatique 1. La carte d'accès réseau 3 est de type connu telle que par exemple éthernet, pour recevoir et émettre des messages circulant sur un réseau informatique. La carte de cryptographie 4 est destinée à coder et décoder des messages sécurisés au moyen de circuits matériels dédiés qui mettent en œuvre des algorithmes de cryptage de type connus tels que par exemple tripleDES. Les circuits matériels dédiés, non représentés, permettent un traitement de codage et décodage plus rapide que des programmes purement logiciels. Ces circuits ne font pas l'objet de la présente invention.

La mémoire 1 comprend des données et des programmes d'une couche utilisateur 5 et d'une couche noyau 6. La couche utilisateur 5 est de type connu pour exécuter des applications telles que des applications clientes ou serveur sur Internet comme http, www, telnet ou autres. La couche noyau 6 est destinée à contenir des structures de données et des fonctions primitives d'un système d'exploitation tel que par exemple le système d'exploitation connu LINUX.

La couche noyau 6 comprend une couche réseau 7 et un pilote 8. La couche réseau 7 est destinée à exécuter des protocoles réseaux tels que par exemple le protocole IP. La couche réseau 7 comprend une couche sécurité 9 destinée à exécuter des protocoles de communication sécurisée tels que par exemple Ipsec. Le pilote 8 est destiné à

commander la carte de cryptographie 4, essentiellement sur demande de la couche sécurité 9.

En référence à la figure 3, dans un état initial 12, la couche sécurité réseau 9 ne consomme aucune ressource du système. Sur détection d'un message à sécuriser, une transition 13, 14, 15, 16 fait passer la couche sécurité réseau respectivement dans un état 17, 18, 19, 20 qui appelle une fonction F1, F2, F3, F4 de traitement du message. Au retour de la fonction appelée F1, F2, F3, F4, une transition 21, 22, 23, 24, signalant que le message est traité, fait repasser la couche sécurité réseau 9 dans l'état initial 12, libérant ainsi les ressources systèmes nécessaires à la couche sécurité réseau 9.

La transition 13 correspond à une détection de message M1 à décrypter. La fonction F1 appelée est une fonction du pilote 8 qui commande à la carte de cryptographie 4 de décrypter le message. La carte de cryptographie est équipée de l'algorithme et des clefs nécessaires au décryptage du message. Par exemple, dans le cas de l'algorithme tripleDES, la carte de cryptographie dispose de la clef secrète pour décoder le message. Lorsque la carte de cryptographie 4 a terminé de décrypter le message, le pilote 8 valide la transition 21 en remettant le message M1 à disposition de la couche sécurité réseau 9.

La transition 14 correspond à une détection de message M2 à authentifier. La fonction F2 appelée est une fonction du pilote 8 qui commande à la carte de cryptographie 4 d'authentifier le message. La carte de cryptographie est équipée de l'algorithme et des clefs nécessaires à l'authentification du message. Par exemple, dans le cas de l'algorithme HMAC-SHA1, la carte de cryptographie dispose de la clef secrète de façon à vérifier la signature de la passerelle 66. Lorsque la carte de cryptographie 4 a terminé d'authentifier le message, le pilote 8 valide la transition 22 en remettant le message M2 à disposition de la couche sécurité réseau 9.

La transition 15 correspond à une détection de message M4 à signer. La fonction F4 appelée est une fonction du pilote 8 qui commande à la carte de cryptographie 4 de signer le message. La carte de cryptographie est équipée de l'algorithme et des clefs nécessaires pour signer le message. Par exemple, dans le cas de l'algorithme HMAC-SHA1, la carte de cryptographie dispose de la clef secrète pour élaborer sa signature.

Lorsque la carte de cryptographie 4 a terminé de signer le message, le pilote 8 valide la transition 21 en remettant le message M4 à disposition de la couche sécurité réseau 9.

La transition 16 correspond à une détection de message M3 à crypter. La fonction F3 appelée est une fonction du pilote 8 qui commande à la carte de cryptographie 4 de crypter le message. La carte de cryptographie est équipée de l'algorithme et des clefs nécessaires au cryptage du message. Par exemple, dans le cas de l'algorithme tripleDES, la carte de cryptographie dispose de la clef secrète pour coder le message. Lorsque la carte de cryptographie 4 a terminé de crypter le message, le pilote 8 valide la transition 24 en remettant le message M3 à disposition de la couche sécurité réseau 9.

L'inconvénient de l'état de la technique ici décrit en référence à la figure 3 est que le traitement du message nécessite d'être terminé pour permettre à la couche sécurité réseau 9 de revenir à l'état initial 12 et libérer les ressources du système ou être disponible pour un traitement ultérieur d'un autre ou du même message. En effet un message qui se présente par exemple comme message M1 à décrypter peut se présenter comme message M2 à authentifier après avoir été décrypté. Toutes les combinaisons sont possibles. Or les traitements de cryptage et de décryptage sont particulièrement longs, même effectués au moyen de circuits matériels.

En référence à la figure 4, dans un état initial 12, la couche sécurité réseau 9 ne consomme aucune ressource du système. Sur détection d'un message M1, M2, M4, M3, auquel appliquer un traitement de sécurité, une transition 13, 14, 15, 16 fait passer la couche sécurité réseau respectivement dans un état 25, 26, 27, 28 qui déclenche une séquence de sauvegarde F5, F6, F7, F8 du contexte d'exécution en cours CE. En fin de séquence F5, F6, F7, F8, une transition 29, 30, 31, 32, est validée par une valeur de pointeur PZS(M1), PZS(M2), PZS(M4), PZS(M3) sur une zone de sauvegarde résultant de l'état précédent 25, 26, 27, 28.

Les traitements de sécurité, décryptage en aval de la transition 13, authentification en aval de la transition 14, signature en aval de la transition 15, cryptage en aval de la transition 16, sont considérés à titre d'exemple non limitatif en référence aux figures 3 et 4, comparativement à la figure 3. L'enseignement de l'invention reste valable pour tout autre traitement tel que résumé (digest en anglais) ou compression de message.

Chaque séquence de sauvegarde F5, F6, F7, F8 est spécifique du traitement à effectuer pour chaque type de message M1, M2, M4, M3. La séquence F5, F6, F7, F8 consiste essentiellement à sauvegarder dans une zone mémoire le contexte d'exécution CE en cours. Le contexte d'exécution CE en cours est constitué de variables locales et globales qui sont utilisées par la couche sécurité réseau 9 pour le traitement du message telles que caractéristiques de sécurité du message, protocoles et clefs à employer. Le début de la zone mémoire est repérée par un pointeur PZS(M1), PZS(M2), PZS(M4), PZS(M3) de façon à ce que le contexte d'exécution CE lié au traitement du message M1, M2, M4, M3, puisse être restitué ultérieurement.

Lorsque la séquence F5 a terminé de sauvegarder le contexte d'exécution CE, la transition 29 fait passer la couche sécurité réseau 9 dans un état 33 qui effectue un appel à une fonction F9 exécutée par le pilote 8 pour commander à la carte 4, un décryptage du message M1. La fonction F9 passe en paramètres, une adresse @F13 de fonction dite de retour, une variable dite de corrélation VC1 et la valeur du pointeur PZS(M1).

Une transition 37 est validée par un acquittement de la fonction F9, retourné par le pilote 8. La transition 37 refait passer la couche sécurité réseau 9 dans son état initial 12.

Lorsque la séquence F6 a terminé de sauvegarder le contexte d'exécution CE, la transition 30 fait passer la couche sécurité réseau 9 dans un état 34 qui effectue un appel à une fonction F10 exécutée par le pilote 8 pour commander à la carte 4, une authentification du message M2. La fonction F10 passe en paramètres, une adresse @F14 de fonction dite de retour, une variable dite de corrélation VC2 et la valeur du pointeur PZS(M2).

Une transition 38 est validée par un acquittement de la fonction F10, retourné par le pilote 8. La transition 38 refait passer la couche sécurité réseau 9 dans son état initial 12.

Lorsque la séquence F7 a terminé de sauvegarder le contexte d'exécution CE, la transition 31 fait passer la couche sécurité réseau 9 dans un état 35 qui effectue un

appel à une fonction F11 exécutée par le pilote 8 pour commander à la carte 4, une signature du message M4. La fonction F11 passe en paramètres, une adresse @F15 de fonction dite de retour, une variable dite de corrélation VC4 et la valeur du pointeur PZS(M4).

Une transition 39 est validée par un acquittement de la fonction F11, retourné par le pilote 8. La transition 39 refait passer la couche sécurité réseau 9 dans son état initial 12.

Lorsque la séquence F8 a terminé de sauvegarder le contexte d'exécution CE, la transition 32 fait passer la couche sécurité réseau 9 dans un état 36 qui effectue un appel à une fonction F12 exécutée par le pilote 8 pour commander à la carte 4, une signature du message M3. La fonction F12 passe en paramètres, une adresse @F16 de fonction dite de retour, une variable dite de corrélation VC3 et la valeur du pointeur PZS(M3).

Une transition 40 est validée par un acquittement de la fonction F12, retourné par le pilote 8. La transition 40 refait passer la couche sécurité réseau 9 dans son état initial 12.

La figure 6 présente des états et transition du pilote 8 de carte de cryptographie particulièrement adaptés pour s'interfacer avec les états et transitions de la couche sécurité réseau 9 conforme à l'invention, en référence aux figures 3 et 4. D'autres états du pilote, applicables à la commande de la carte 4, ne sont pas décrits ici car ces autres états sortent du cadre de la présente invention. Les états décrits sont ceux qui correspondent aux traitement de cryptage et de décryptage. L'enseignement qui en résulte est applicable à l'authentification, la signature et ou à tout autre traitement de sécurisation tel que le résumé de message au moyen de la carte matérielle 4.

Dans un état initial 41, le pilote 8 n'utilise aucune ressource du système. Une transition 42 est activée par l'appel de la fonction F9, effectué dans l'état 33 de la couche sécurité réseau 9. Une transition 43 est activée par l'appel de la fonction F12, effectué dans l'état 36 de la couche sécurité réseau 9.

La transition 42 fait passer le pilote 8 dans un état 44. Dans l'état 44, le pilote 8 envoie immédiatement acquittement Acq(F9) qui valide la transition 37 et active la carte 4 pour effectuer un traitement matériel de décryptage du message M1. La carte 4 prend alors en charge le message M1. Dès que la carte 4 est activée, une transition 46 refait passer le pilote dans l'état initial 41 qui le rend disponible pour prendre en charge d'autres demandes de traitement par la couche de sécurité réseau 9.

Lorsque la carte 4 a terminé de décrypter le message M1, une transition 48 fait passer le pilote dans un état 50. Dans l'état 50, le pilote effectue un branchement sur l'adresse @F13 de fonction de retour en communiquant le pointeur PZS(M1) précédemment donnés dans l'état 33 de la couche de sécurité réseau. Le pilote place également dans la variable de corrélation VC1, les coordonnées de mise à disposition du message M1 décrypté par la carte 4. Puis le pilote retourne dans son état initial 41.

La transition 43 fait passer le pilote 8 dans un état 45. Dans l'état 45, le pilote 8 envoie immédiatement acquittement Acq(F12) qui valide la transition 40 et active la carte 4 pour effectuer un traitement matériel de cryptage du message M3. La carte 4 prend alors en charge le message M3. Dès que la carte 4 est activée, une transition 47 refait passer le pilote dans l'état initial 41 qui le rend disponible pour prendre en charge d'autres demandes de traitement par la couche de sécurité réseau 9.

Lorsque la carte 4 a terminé de crypter le message M3, une transition 49 fait passer le pilote dans un état 51. Dans l'état 51, le pilote effectue un branchement sur l'adresse @F16 de fonction de retour en communiquant le pointeur PZS(M3) précédemment donnés dans l'état 36 de la couche de sécurité réseau. Le pilote place également dans la variable de corrélation VC3, les coordonnées de mise à disposition du message M3 crypté par la carte 4. Puis le pilote retourne dans son état initial 41.

En référence à la figure 5, une transition 52 fait passer la couche sécurité réseau de l'état initial 12 à un état 56, une transition 53 fait passer la couche sécurité réseau de l'état initial 12 à un état 57, une transition 54 fait passer la couche sécurité réseau de l'état initial 12 à un état 58, une transition 55 fait passer la couche sécurité réseau de l'état initial 12 à un état 59.

La transition 52 est validée par le branchement sur l'adresse @F13 et la communication du pointeur PZS(M1) effectués dans l'état 50. Dans l'état 56, la couche de sécurité réseau 9 restitue le contexte d'exécution sauvegardé dans la zone mémoire pointée par PZS(M1). La couche de sécurité réseau 9 se replace ainsi dans la configuration dans laquelle elle était lorsqu'elle était dans l'état 25 pour le message M1 alors que le message M1 n'était pas décrypté. Cependant, le message étant à présent décrypté, la variable de corrélation VC1 valide immédiatement une transition 60 qui replace la couche de sécurité réseau dans son état initial 12. La variable de corrélation VC1 met le message M1 à disposition de la couche de sécurité réseau 9 pour mise à disposition d'autres fonctions de la couche réseau ou pour présenter le message M1 traité comme message de type M2, M3, M4 pour un autre traitement. Pour mettre le message M1 à disposition de la couche de sécurité réseau 9, la valeur de la variable de corrélation VC1 est par exemple une valeur permettant de reprendre l'exécution à un endroit adéquat.

La transition 55 est validée par le branchement sur l'adresse @F16 et la communication du pointeur PZS(M3) effectués dans l'état 51. Dans l'état 59, la couche de sécurité réseau 9 restitue le contexte d'exécution sauvegardé dans la zone mémoire pointée par PZS(M3). La couche de sécurité réseau 9 se replace ainsi dans la configuration dans laquelle elle était lorsqu'elle était dans l'état 28 pour le message M3 alors que le message M3 n'était pas crypté. Cependant, le message étant à présent crypté, la variable de corrélation VC3 valide immédiatement une transition 64 qui replace la couche de sécurité réseau dans son état initial 12. La variable de corrélation VC3 met le message M3 à disposition de la couche de sécurité réseau 9 pour mise à disposition d'autres fonctions de la couche réseau 7 ou pour présenter le message M3 traité comme message de type M2, M1, M4 pour un autre traitement.

De même, la transition 53 est validée par le branchement sur l'adresse @F14 et la communication du pointeur PZS(M2) effectués dans un état non représenté du pilote 8. Dans l'état 57, la couche de sécurité réseau 9 restitue le contexte d'exécution sauvegardé dans la zone mémoire pointée par PZS(M2). La couche de sécurité réseau 9 se replace ainsi dans la configuration dans laquelle elle était lorsqu'elle était dans l'état 26 pour le message M2 alors que le message M2 n'était pas authentifié. Cependant, le message étant à présent authentifié, la variable de corrélation VC2 valide immédiatement une transition 62 qui replace la couche de sécurité réseau dans son état

initial 12. La variable de corrélation VC2 met le message M2 à disposition de la couche de sécurité réseau 9 pour mise à disposition d'autres fonctions de la couche réseau 7 ou pour présenter le message M2 traité comme message de type M1, M3, M4 pour un autre traitement.

De même, la transition 54 est validée par le branchement sur l'adresse @F15 et la communication du pointeur PZS(M4) effectués dans un état non représenté du pilote 8. Dans l'état 58, la couche de sécurité réseau 9 restitue le contexte d'exécution sauvegardé dans la zone mémoire pointée par PZS(M4). La couche de sécurité réseau 9 se replace ainsi dans la configuration dans laquelle elle était lorsqu'elle était dans l'état 27 pour le message M4 alors que le message M2 n'était pas signé. Cependant, le message étant à présent signé, la variable de corrélation VC4 valide immédiatement une transition 63 qui replace la couche de sécurité réseau dans son état initial 12. La variable de corrélation VC4 met le message M4 à disposition de la couche de sécurité réseau 9 pour mise à disposition d'autres fonctions de la couche réseau 7 ou pour présenter le message M4 traité comme message de type M1, M3, M2 pour un autre traitement.

Prenons sur la figure 2 un cheminement 10 de message crypté M1 de la carte réseau 3 à la carte de cryptographie 4 suivi d'un cheminement 11 du message décrypté M1 de la carte 4 à la mémoire 2 pour sa présentation par exemple à la couche utilisateur 5.

Lorsque le message M1 en provenance de la carte 3 est transmis à la mémoire 2 selon la branche ascendante du cheminement 10, sa présentation à la couche de sécurité réseau 9 valide la transition 13. La couche de sécurité réseau 9 reste peu de temps dans l'état 25 car la sauvegarde du contexte d'exécution est une opération relativement rapide. A la suite de l'état 25, la couche de sécurité réseau 9 reste peu de temps dans l'état 33 car l'état 44 du pilote 8 envoie l'acquittement Acq(F9) immédiatement après l'appel de la fonction F9 sans attendre que le message M1 soit décrypté. La couche de sécurité réseau 9 retourne donc rapidement dans son état initial 12. D'une part, ceci évite au système de rester bloqué pendant le traitement de décryptage du message M1 car ce traitement est pris en charge par la carte 4 de façon asynchrone. D'autre part, ceci présente l'avantage de rendre la couche de sécurité réseau rapidement à nouveau disponible pour une présentation d'un autre message à traiter.

Lorsque le message M1 est rangé décrypté par la carte 4 en mémoire 2 selon une première branche ascendante du cheminement 11, l'état 50 du pilote 8 valide la transition 52 de la couche sécurité réseau 9. La couche de sécurité réseau 9 reste peu de temps dans l'état 56 qui en résulte, car la restitution du contexte d'exécution CE est une opération relativement rapide. En fin de restitution de contexte CE, la transition 21 replace rapidement la couche de sécurité réseau 9 dans l'état initial 12 car la valeur de corrélation VC1 met immédiatement le message M1 sous forme décryptée à disposition de la couche sécurité réseau 9 pour être retransmis, dans le cas de la figure 2, à la couche utilisateur 5 selon une deuxième branche ascendante du cheminement 11. Ainsi, le temps de décryptage du message M1 est totalement transparent pour la couche de sécurité réseau 9, activée seulement un court instant après présentation du message M1 à décrypter, puis réactivée seulement un court instant après présentation du message M1 décrypté. Les cheminements 10 et 11 de la figure 2 sont symboliques dans le but uniquement de montrer l'intérêt de l'invention. L'homme du métier sait par ailleurs qu'une ou plusieurs couches peuvent séparer la couche réseau 7 de la couche utilisateur 5, telle qu'une couche transport de type connu TCP, non représentée de façon à ne pas surcharger inutilement la figure 2. D'autre part, le cheminement 11 peut aussi être redirigé vers la carte 3 par la couche réseau 7 ou à nouveau vers la carte 4 pour un traitement subséquent.

Comme la couche noyau 6 n'est pas bloquée en attente de fin de traitement d'un message, il est intéressant de faire prendre en charge d'autres messages qui se présentent à la couche sécurité réseau 9 alors qu'un premier message n'est pas encore terminé d'être traité.

En référence à la figure 7, pendant que le message M1 est pris en charge par la carte 4 pour être décrypté, le pointeur PZS(M1) a pour valeur celle d'un mot 56 qui contient une adresse de début d'une zone 52 de la mémoire 2. La zone 52 contient le contexte d'exécution CE lorsque la couche sécurité réseau était dans l'état 25 pour le message M1. Un mot 55 est destiné à contenir une adresse suivant une dernière adresse de la zone 52. Ainsi, le mot 55 définit un pointeur de zone libre PZL sur une zone de sauvegarde de contexte d'exécution suivante 53.

Lorsqu'un autre message M'1 se présente à la couche de sécurité réseau 7, la valeur du mot 55 est transférée dans un mot 57 pour définir un nouveau pointeur PZS(M'1) sur le début de la zone 53 où est sauvegardé le contexte d'exécution CE lorsque la couche sécurité réseau est dans l'état 25 pour le message M'1. Le mot 55 est contient alors une adresse suivant une dernière adresse de la zone 53. Ainsi, le mot 55 définit un pointeur de zone libre PZL sur une zone de sauvegarde de contexte d'exécution suivante 54, disponible pour le contexte d'exécution CE lié à un nouveau message M"1. Ce processus est répété pour tout nouveau message de façon à chaîner les sauvegardes de contexte d'exécution CE.

Suite à une restitution de contexte d'exécution CE dans l'état 56 de la couche de sécurité réseau, l'adresse de début de la zone de sauvegarde libérée est prise comme adresse suivante de la dernière zone de sauvegarde occupée selon un mécanisme de chaînage classique.

Il est possible d'utiliser une structure de données semblable à celle qui vient d'être décrite, distincte pour chacun des états 25, 26, 27, 28 de la couche de sécurité réseau, ou commune à tous les états 25, 26, 27, 28, auquel cas les mots 56, 57 peuvent contenir des PZS(M1), PZS(M2), PZS(M3), PZS(M4) pour l'un quelconque de ces états.

La couche de sécurité réseau peut être programmée de différentes manières pour mettre en œuvre les états précédemment décrits. Un procédé de réalisation de code de la couche de sécurité réseau 9 à partir d'une couche de sécurité réseau standard telle que par exemple la couche Ipsec de LINUX, comprend essentiellement deux étapes.

La première étape est expliquée en référence à la figure 8. Dans la couche noyau 6 du dispositif informatique 1, une première séquence de code 75 est destinée à être activée par une présentation de message M1, M2, M3 ou M4 auquel appliquer un traitement de sécurisation, décryptage, authentification, cryptage ou signature. Dans la couche de sécurité réseau standard, la séquence de code 75 est constituée de plusieurs lignes de code standard qui ne font pas l'objet de la présente invention. On distingue à ce stade uniquement une ligne 76 et une dernière ligne de la séquence 75 repérée par un indicateur de Fin. La ligne 76 contient un appel à la fonction de traitement de

sécurisation standard, par exemple la première fonction F1 si la séquence de code 75 est celle activée par la présentation du message M1.

La première séquence de code 75 est modifiée en insérant avant la ligne 75, une deuxième séquence de code 77. La séquence de code 77 commence par une ou plusieurs lignes F5(CE) qui sauvegardent le contexte d'exécution CE en cours lorsque la première séquence est activée, c'est à dire essentiellement les valeurs des variables locales et globales utilisées dans la séquence de code 75. Le code de sauvegarde consiste alors en des écritures des valeurs de ces variables dans une zone de la mémoire 2, repérée par le pointeur PZS(M1).

A la suite des lignes F5(CE), la séquence 77 contient le code d'appel à une deuxième fonction de sécurisation, par exemple la fonction F9(@F13, VC1, PZS(M1)) dans le cas ici décrit. La deuxième fonction est destinée à être exécutée par le pilote 8. Les paramètres passés sont essentiellement une adresse de fonction @F13 et le pointeur PZS sur la zone de sauvegarde.

La séquence de code 77 se termine par un branchement sur la dernière ligne de la séquence de code 75 de type "Goto Fin".

La deuxième étape est expliquée en référence à la figure 9. La première séquence de code 75 est copiée de façon à générer une troisième séquence de code 78, prise comme étant le code de la fonction F13 dont l'adresse @F13 est repérée par un pointeur 81. Une quatrième séquence de code 80 est insérée après la ligne 76 de la séquence 78. La séquence 80 est repérée par une étiquette et contient des instructions de lecture de la zone mémoire indiquée par le pointeur PZS. Une ligne 79 est insérée en début de séquence 78. La ligne 79 contient une instruction de branchement "Goto Etiquette" sur la séquence de code 80.

La couche de sécurité réseau (9) obtenue par le procédé précédemment décrit, est plus rapide que la couche de sécurité réseau standard d'origine. En effet, dans la couche de sécurité standard, l'exécution de la séquence 75 non modifiée s'effectue de la façon suivante. Les instructions de code standard qui précèdent la ligne 76 sont exécutées. La ligne 76 effectue un appel à la fonction de traitement standard F1. Les instructions de

code standard suivant la ligne 76 sont exécutées après le retour de la fonction F1 qui indique la fin de traitement du message. Or un traitement de cryptographie est long par nature. Ceci a pour effet de retarder l'atteinte en exécution de la dernière ligne "Fin" de la séquence 75 non modifiée.

Dans la couche de sécurité réseau obtenue par le procédé, l'exécution de la séquence 75 modifiée s'effectue de la façon suivante. Les instructions de code standard qui précèdent la ligne 76 et la séquence 77 sont exécutées. La ligne 76 et les lignes suivantes de la séquence 75 ne sont jamais exécutées à cause du premier branchement sur la dernière ligne de la séquence 75. Le premier branchement est effectué rapidement car la fonction F9 envoie immédiatement un acquittement avant que le message ne soit terminé d'être traité. Lorsque le traitement du message est terminé, le pilote 8 déclenche une exécution de la séquence de code 78 au moyen de l'adresse @F13. La ligne de code 76 et les lignes de code de la séquence 78 qui précèdent ne sont jamais exécutées à cause du branchement en début de séquence 78 sur la séquence 80 qui permet l'exécution des lignes de code suivantes, masquant ainsi le temps de traitement du message.

Le dispositif informatique qui vient d'être décrit permet de mettre en œuvre un procédé d'obtention d'un message sécurisé à partir d'un autre message.

En référence à la figure 10, sur présentation dudit autre message à la couche de sécurité réseau, dans une première étape 82, le contexte d'exécution en cours est sauvegardé. Cette étape est réalisée dans l'un des états 25, 26, 27, 28 de la couche 9. Dans une deuxième étape 83, une requête de traitement de sécurisation est émise depuis la couche 9, dans l'un des états 33, 34, 35, 36, vers un élément extérieur à la couche 9, de façon à ce que la couche 9 soit remise dans son état initial qui n'utilise aucune ressource du dispositif. Les étapes 82 et 83 sont mises en œuvre au moyen de la séquence 77. Après que l'élément extérieur ait traité ledit autre message, le contexte sauvegardé est restitué dans une étape 84 de façon à produire le message sécurisé.

Ce procédé présente l'avantage de pouvoir produire des messages sécurisés en grand nombre car l'étape 84 peut être activée après plusieurs activations successives des étapes 82, 83 pour différents messages.

REVENDICATIONS:

1. Dispositif informatique (1) comprenant une mémoire (2) et une couche de sécurité réseau (9) pour appliquer un traitement de sécurisation sur présentation d'un message (M1) dans la mémoire (2), caractérisé en ce que:
- la présentation du message (M1) fait passer la couche de sécurité réseau (9) d'un état initial (12) à un premier état (25) qui réalise une sauvegarde de contexte d'exécution (CE) dans une zone (52) de la mémoire (2);
- la réalisation de la sauvegarde du contexte d'exécution (CE), fait passer la couche de sécurité réseau du premier état (25) à un deuxième état (33) qui appelle une première fonction (F9) de traitement du message (M1), en passant comme paramètres de ladite première fonction (F9), au moins une adresse (@F13) de deuxième fonction (F13) et un pointeur PZS(M1) sur la zone (52) de la mémoire (2);
- un acquittement de la première fonction (F9) avant traitement du message (M1), fait immédiatement repasser la couche de sécurité réseau dans l'état initial (12);
- un branchement sur l'adresse (@F13) de deuxième fonction, fait passer la couche de sécurité réseau (9) de l'état initial (12) à un troisième état (56) qui réalise une restitution du contexte d'exécution (CE) avant de faire repasser la couche de sécurité réseau (9) dans l'état initial.

2. Dispositif informatique (1) selon la revendication 1, caractérisé en ce que plusieurs pointeurs PZS(M1), PZS(M'1) sont chaînés de façon à pouvoir être restitués lors du branchement sur ladite adresse (@F13).

3. Dispositif informatique (1) selon la revendication 1 ou 2, caractérisé en ce que l'appel de la première fonction (F9) fait passer comme paramètre une variable de corrélation (VC1), restituée lors du branchement sur l'adresse (@F13).

4. Procédé de réalisation de code d'une couche rapide de sécurité réseau (9) à partir de code d'une couche standard de sécurité réseau dans une couche noyau (6) d'un dispositif informatique (1), caractérisé en ce qu'il comprend:
- une première étape pour modifier dans le code de ladite couche standard, une première séquence de code destinée à être activée par une présentation de message auquel appliquer un traitement de sécurisation, en insérant dans la première séquence,

avant un appel à une première fonction de sécurisation (F1), une deuxième séquence de code qui:

- commence par une sauvegarde d'un contexte d'exécution (CE) en cours lorsque la première séquence est exécutée,
- fait un appel à une deuxième fonction de sécurisation (F9),
- termine par un premier branchement sur la fin de la première séquence de code;

- une deuxième étape pour générer une troisième séquence de code d'une troisième fonction (F13) en copiant ladite première séquence de code modifiée puis en insérant dans ladite troisième séquence de code:

- après l'appel à la première fonction (F1), une quatrième séquence de code de restitution du contexte d'exécution (CE) sauvegardé,
- en début de troisième séquence, un deuxième branchement sur ladite quatrième séquence de code.

5. Procédé pour obtenir un message sécurisé à partir d'un autre message, au moyen d'un dispositif informatique (1) comprenant une couche de sécurité réseau (9) à laquelle est présenté ledit autre message, caractérisé en ce qu'il comprend:

- une première étape pour sauvegarder un contexte d'exécution de la couche de sécurité réseau après présentation du dit autre message;
- une deuxième étape dans laquelle la couche de sécurité réseau émet une requête de traitement de sécurisation vers un élément extérieur à la couche de sécurité réseau telle que ledit élément extérieur acquitte immédiatement cette requête de façon à mettre la couche de sécurité réseau dans un état initial qui n'utilise aucune ressource du dispositif informatique (1);
- une troisième étape dans laquelle ledit élément extérieur active une restitution du contexte d'exécution sauvegardé dans la couche de sécurité réseau en présentant le message sécurisé par le traitement de sécurisation qui résulte de ladite requête.

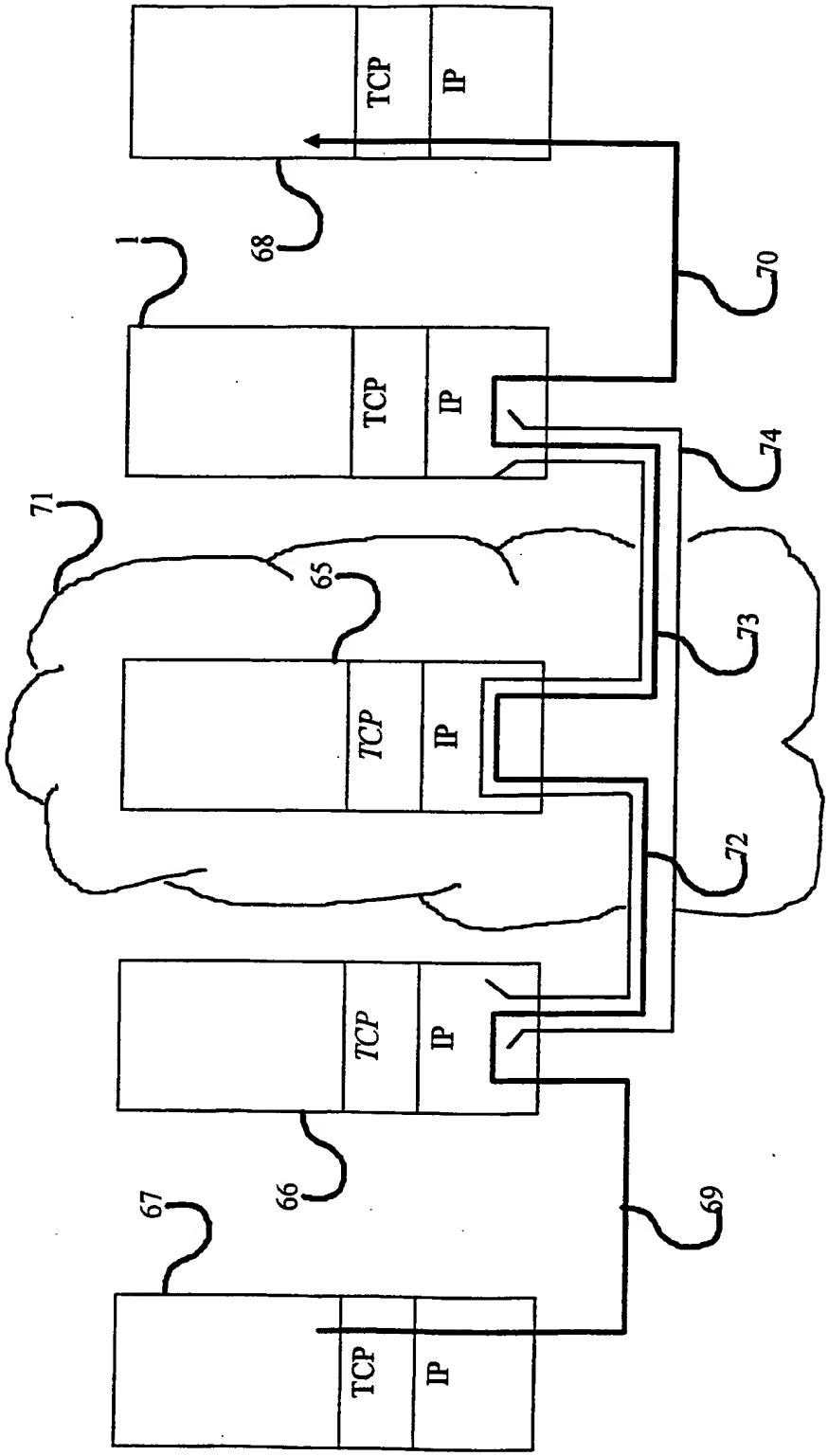
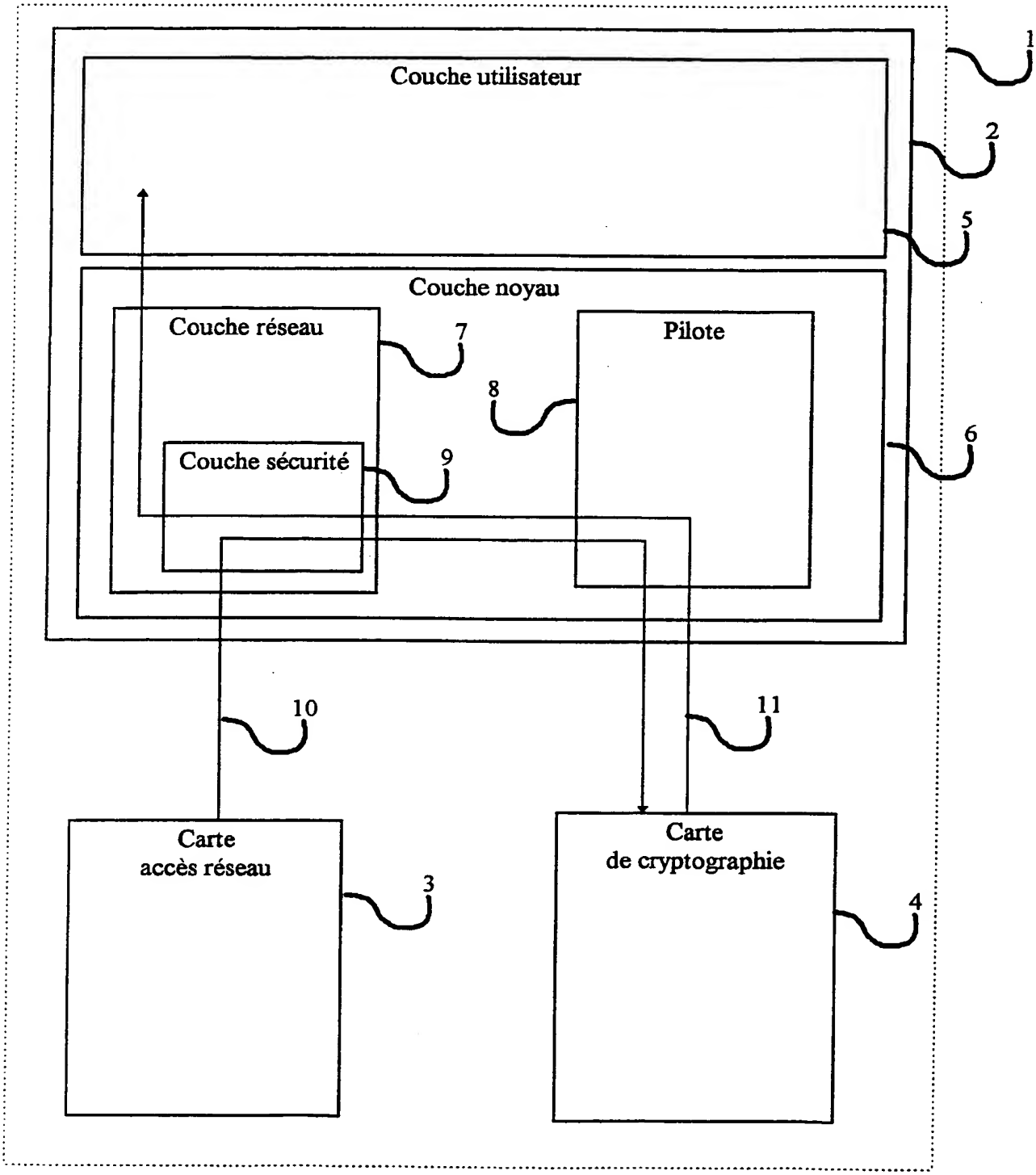


Fig.1

Fig.2


1
Couche utilisateur
2
5
Couche noyau
Couche réseau
7
Pilote
8
6
Couche sécurité
9
10
11
Carte
accès réseau
3
Carte
de cryptographie
4

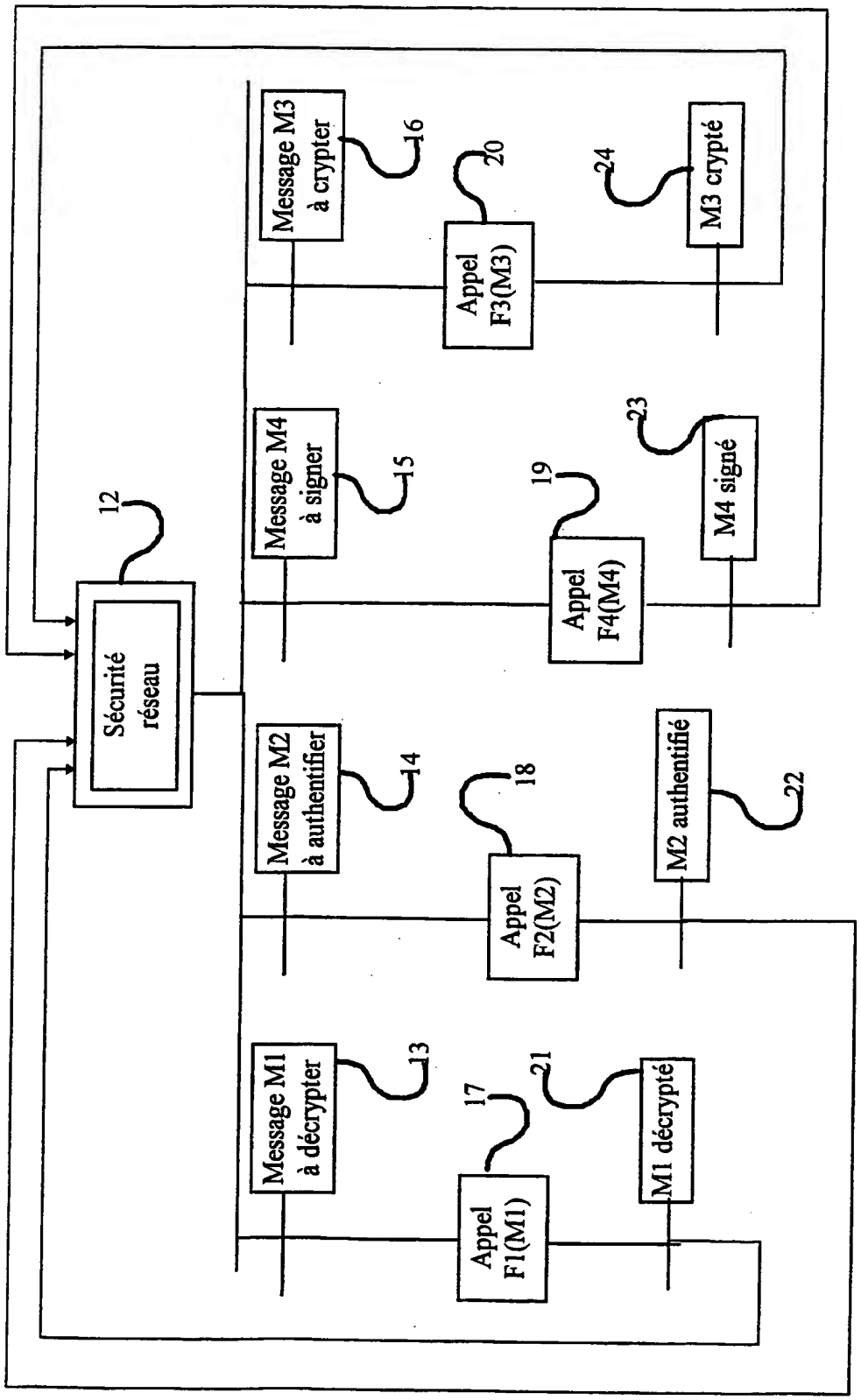

Sécurité réseau
12
Message M1 à décrypter
13
Message M2 à authentifier
14
Message M4 à signer
15
Message M3 à crypter
16
Appel F1(M1)
17
Appel F2(M2)
18
Appel F4(M4)
19
Appel F3(M3)
20
M1 décrypté
21
M2 authentifié
22
M4 signé
23
M3 crypté
24

Fig.3

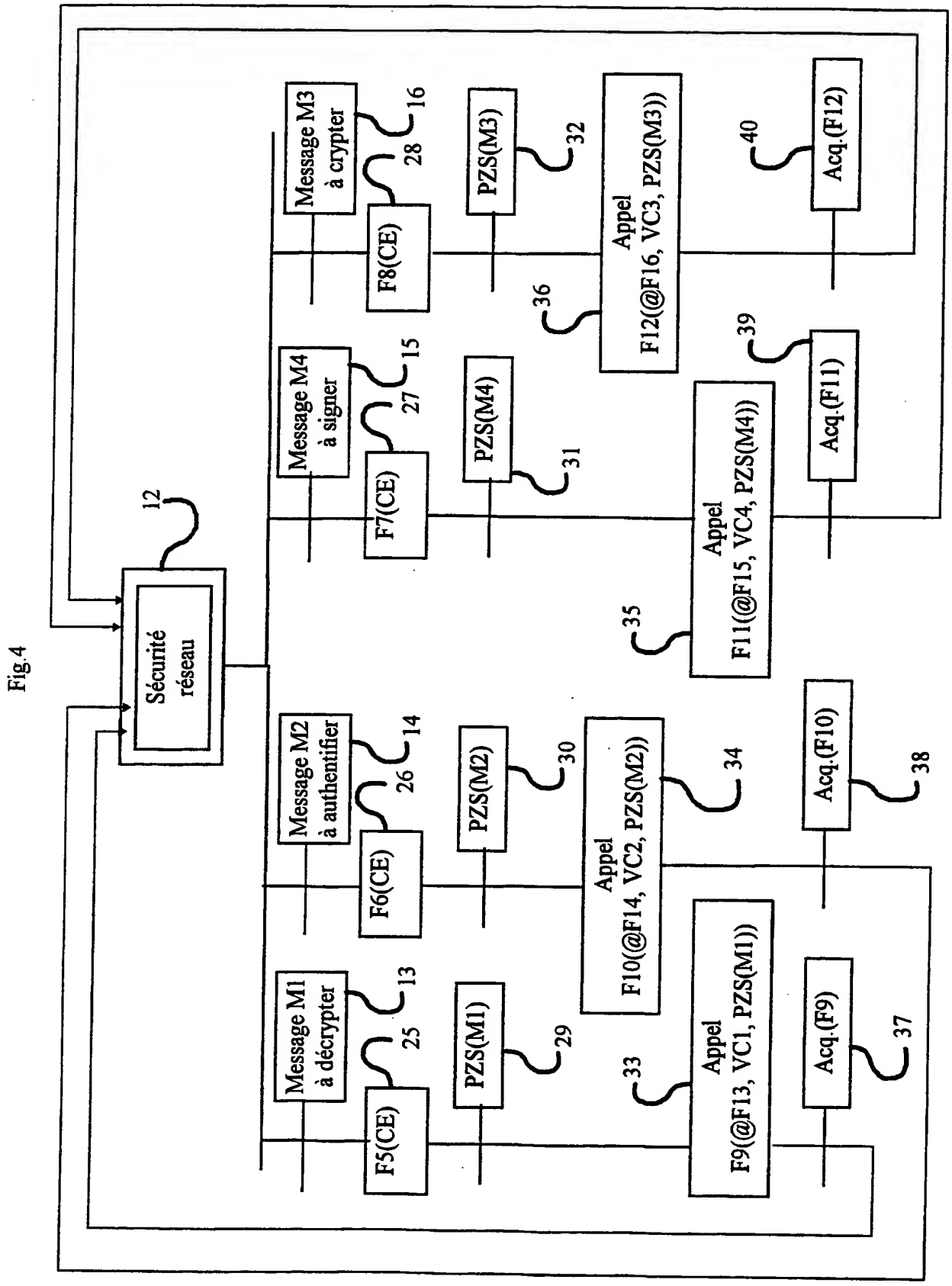

Sécurité réseau
12
Message M1 à décrypter
13
25
F5(CE)
PZS(M1)
29
Message M2 à authentifier
14
26
F6(CE)
PZS(M2)
30
Message M3 à crypter
16
28
F8(CE)
PZS(M3)
32
Message M4 à signer
15
27
F7(CE)
PZS(M4)
31
Appel F9(@F13, VC1, PZS(M1))
33
Appel F10(@F14, VC2, PZS(M2))
34
Appel F11(@F15, VC4, PZS(M4))
35
Appel F12(@F16, VC3, PZS(M3))
36
Acq.(F9)
37
Acq.(F10)
38
Acq.(F11)
39
Acq.(F12)
40

Fig.4

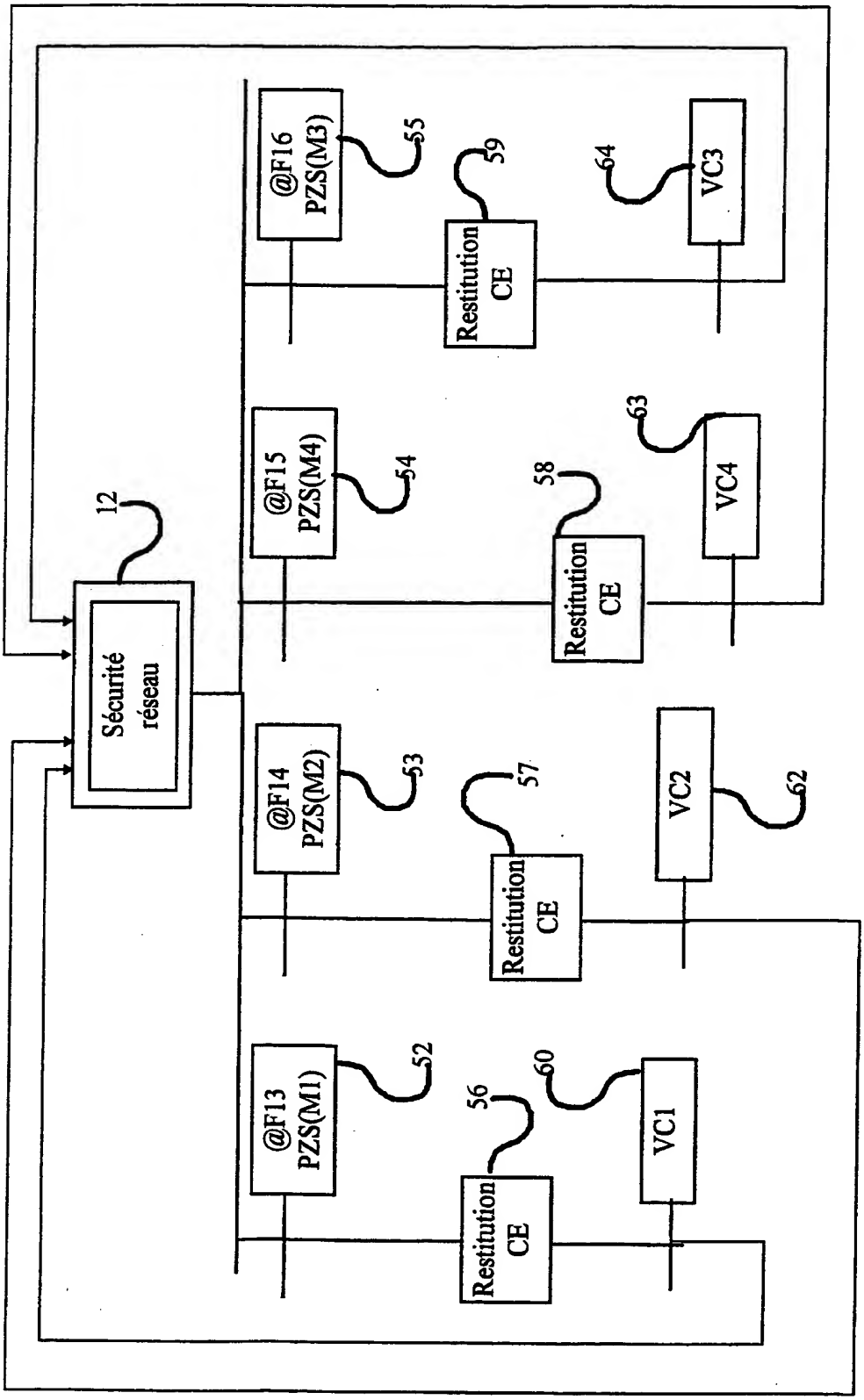

Sécurité réseau
12
@F13 PZS(M1)
52
@F14 PZS(M2)
53
@F15 PZS(M4)
54
@F16 PZS(M3)
55
Restitution CE
56
Restitution CE
57
Restitution CE
58
Restitution CE
59
VC1
60
VC2
62
VC4
63
VC3
64

Fig.5

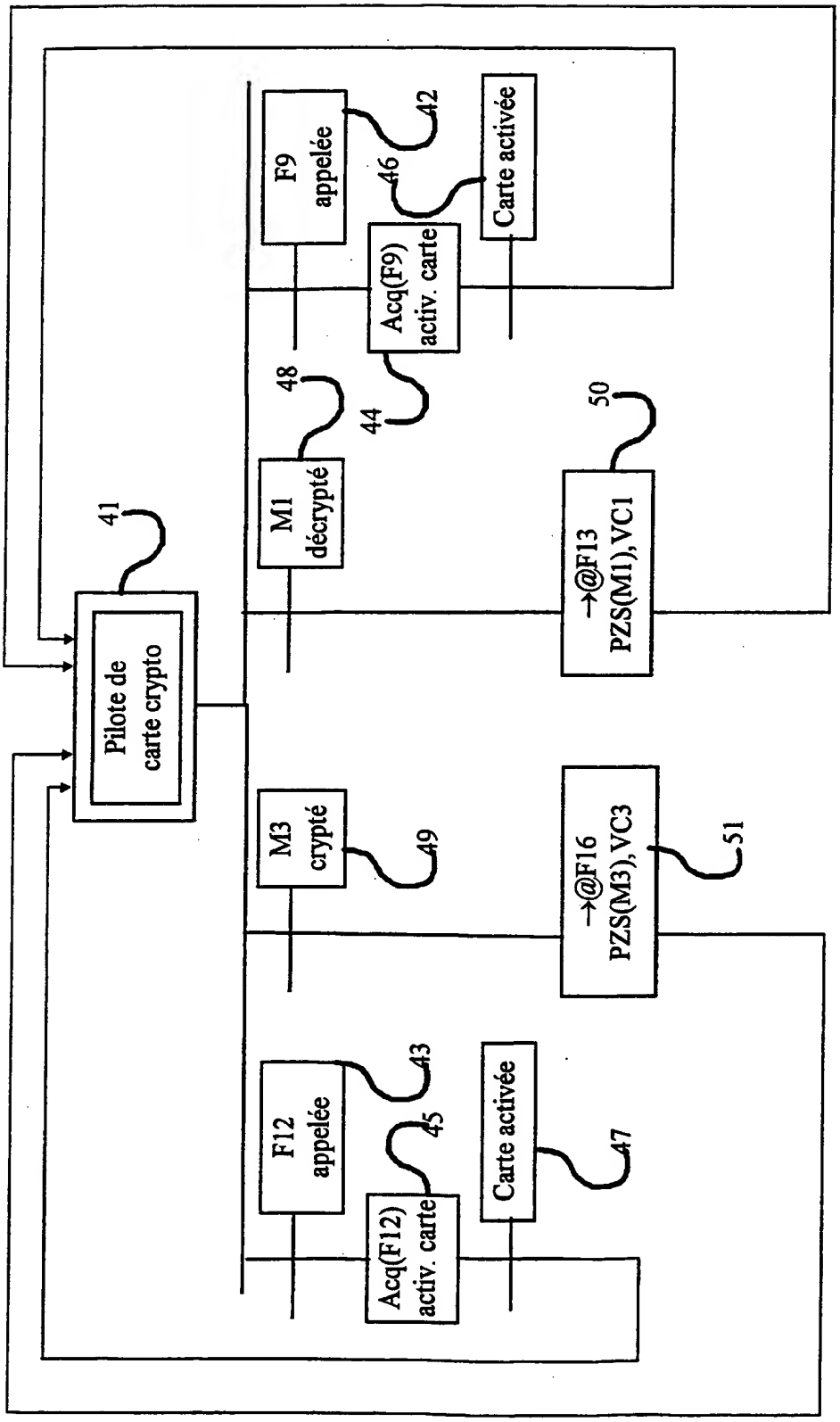

Pilote de carte crypto
41
F9 appelée
42
Carte activée
46
Acq(F9) activ. carte
44
M1 décrypté
48
→@F13 PZS(M1),VC1
50
M3 crypté
49
→@F16 PZS(M3),VC3
51
F12 appelée
43
Acq(F12) activ. carte
45
Carte activée
47

Fig.6

Fig.7

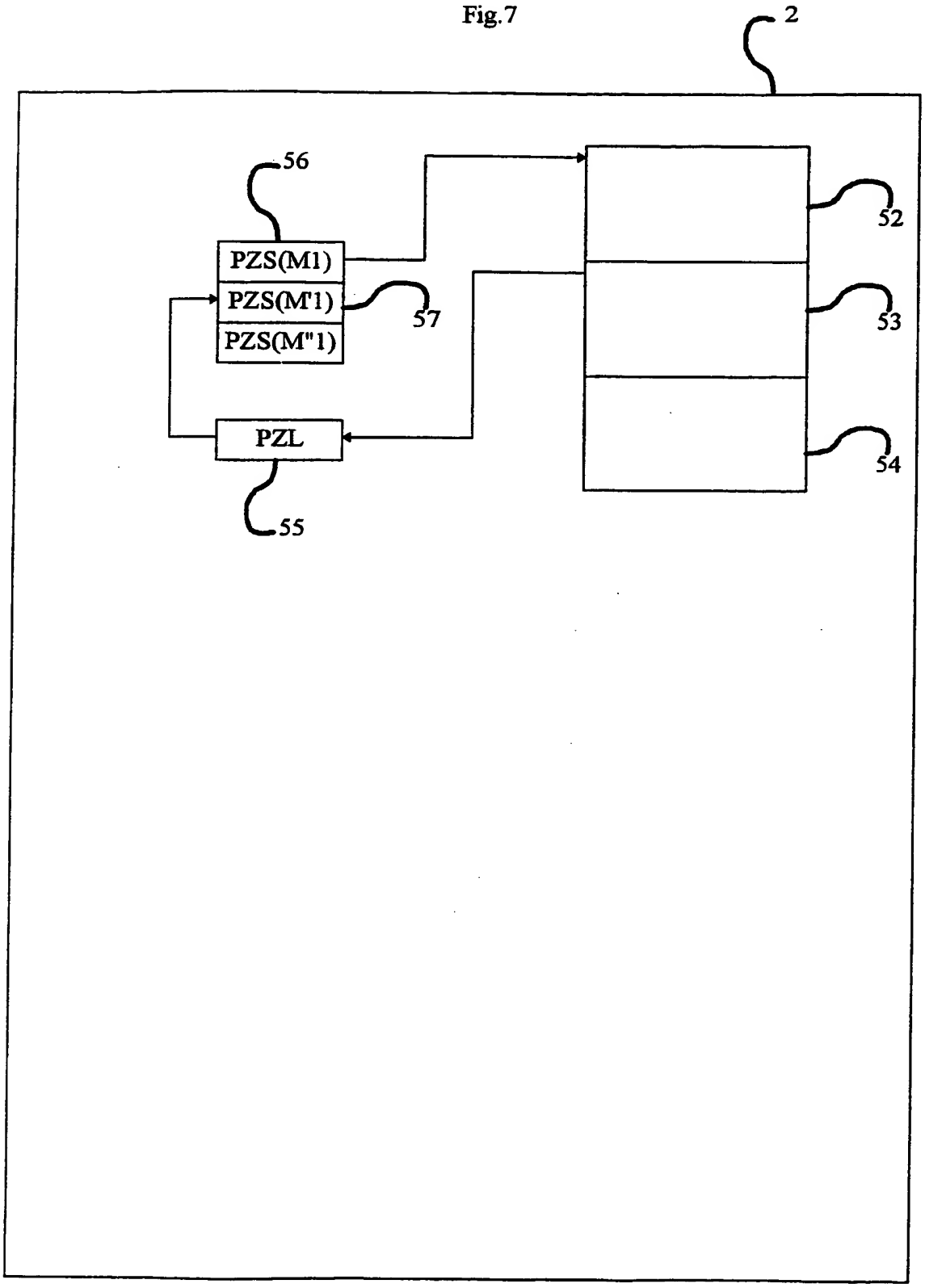


Fig.8

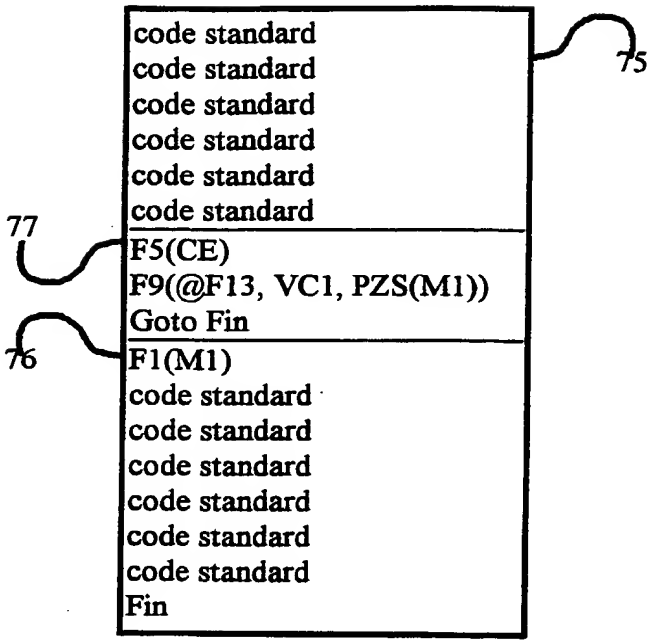

code standard
code standard
code standard
code standard
code standard
code standard
75
77
F5(CE)
F9(@F13, VC1, PZS(M1))
Goto Fin
76
F1(M1)
code standard
code standard
code standard
code standard
code standard
code standard
Fin

Fig.9

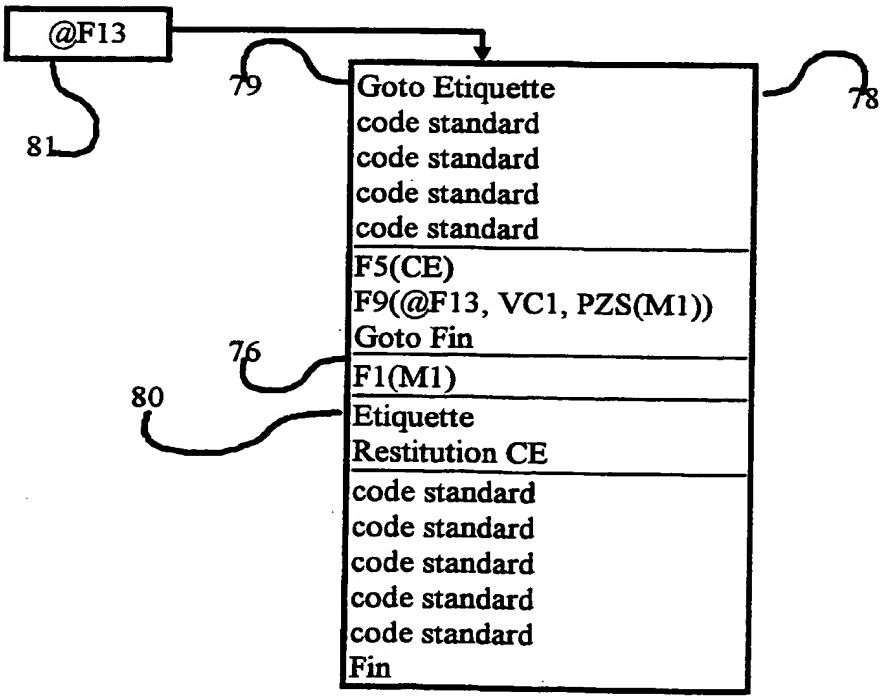
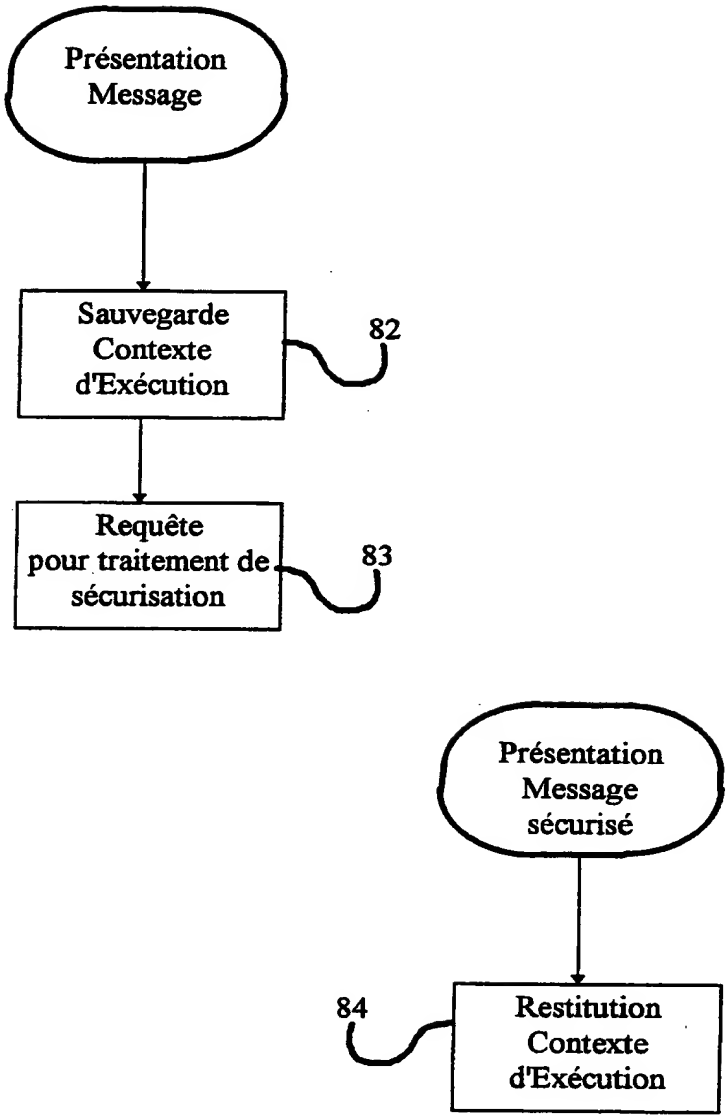

@F13
79
81
Goto Etiquette
code standard
code standard
code standard
code standard
78
F5(CE)
F9(@F13, VC1, PZS(M1))
Goto Fin
76
F1(M1)
80
Etiquette
Restitution CE
code standard
code standard
code standard
code standard
code standard
Fin

Fig. 10


Présentation Message
Sauvegarde Contexte d'Exécution
82
Requête pour traitement de sécurisation
83
Présentation Message sécurisé
84
Restitution Contexte d'Exécution

INTERNATIONAL SEARCH REPORT

International Application No
PCT/FR 00/03230

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06 G06F9/46

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ, INSPEC, IBM-TDB, COMPENDEX

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 485 579 A (LAU JAMES ET AL) 16 January 1996 (1996-01-16) column 12, line 62 -column 14, line 39 column 19, line 32 -column 20, line 7 column 21, line 31-44 column 26, line 11-41 ---	1-5
A	EP 0 942 369 A (LUCENT TECHNOLOGIES INC) 15 September 1999 (1999-09-15) column 4, line 20-41 column 7, line 55 -column 10, line 5 --- -/--	1-5

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
30 March 2001	06/04/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Lázaro, M.I.

1

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	HUNT R: "Internet/Intranet firewall security-policy, architecture and transaction services" COMPUTER COMMUNICATIONS,GB,BUTTERWORTHS & CO. PUBLISHERS LTD, vol. 21, no. 13, 1 September 1998 (1998-09-01), pages 1107-1123, XP004146571 ISSN: 0140-3664 page 1117, line 31 -page 1118, line 10 page 1120, line 38 -page 1121, line 14 figure 11 ---	1-5
A	LIU Y ET AL: "OSI remote procedure call: Standardization issues, design and implementation" COMPUTER COMMUNICATIONS,NL,ELSEVIER SCIENCE PUBLISHERS BV, AMSTERDAM, vol. 20, no. 6, 25 July 1997 (1997-07-25), pages 462-474, XP004126700 ISSN: 0140-3664 page 466, line 18 -page 468, line 37 -----	1-5

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

In ational Application No
PCT/FR 00/03230

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5485579 A	16-01-1996	US 6065037 A	16-05-2000
		AT 179811 T	15-05-1999
		AU 651321 B	21-07-1994
		AU 6436190 A	18-04-1991
		CA 2066566 A	09-03-1991
		DE 69033092 D	10-06-1999
		EP 0490980 A	24-06-1992
		IL 95449 A	07-10-1994
		JP 2945757 B	06-09-1999
		JP 5502127 T	15-04-1993
		KR 201772 B	15-06-1999
		WO 9104540 A	04-04-1991
EP 0942369 A	15-09-1999	CN 1233016 A	27-10-1999
		JP 11296389 A	29-10-1999

PCT

REQUÊTE

Le soussigné requiert que la présente demande internationale soit traitée conformément au Traité de coopération en matière de brevets.

Réservé à l'office récepteur

Demande internationale n°

Date du dépôt international

Nom de l'office récepteur et "Demande internationale PCT"

Référence du dossier du déposant ou du mandataire *(facultatif)* *(12 caractères au maximum)*: **PCT 3876 JMD**

Cadre n° I TITRE DE L'INVENTION

Dispositif informatique pour sécuriser des messages au niveau d'une couche réseau.

Cadre n° II DÉPOSANT

Nom et adresse : *(Nom de famille suivi du prénom; pour une personne morale, désignation officielle complète. L'adresse doit comprendre le code postal et le nom du pays. Le pays de l'adresse indiquée dans ce cadre est l'État où le déposant a son domicile si aucun domicile n'est indiqué ci-dessous.)*

BULL S.A.
68, route de Versailles
78430 LOUVECIENNES
FRANCE

☐ Cette personne est aussi inventeur.

n° de téléphone: 33 (1) 39.66.61.71

n° de télécopieur: 33 (1) 39.66.61.73

n° de téléimprimeur:

Nationalité (nom de l'État) : FRANCE

Domicile (nom de l'État) : FRANCE

Cette personne est déposant pour : ☐ tous les États désignés ☒ tous les États désignés sauf les États-Unis d'Amérique ☐ les États-Unis d'Amérique seulement ☐ les États indiqués dans le cadre supplémentaire

Cadre n° III AUTRE(S) DÉPOSANT(S) OU (AUTRE(S)) INVENTEUR(S)

Nom et adresse : *(Nom de famille suivi du prénom; pour une personne morale, désignation officielle complète. L'adresse doit comprendre le code postal et le nom du pays. Le pays de l'adresse indiquée dans ce cadre est l'État où le déposant a son domicile si aucun domicile n'est indiqué ci-dessous.)*

CUNCHON François
5, rue Claude Nicolas Ledoux
78114 MAGNY LES HAMEAUX
FRANCE

Cette personne est :

☐ déposant seulement

☒ déposant et inventeur

☐ inventeur seulement *(Si cette case est cochée, ne pas remplir la suite.)*

Nationalité (nom de l'État) : FRANCE

Domicile (nom de l'État) : FRANCE

Cette personne est déposant pour : ☐ tous les États désignés ☐ tous les États désignés sauf les États-Unis d'Amérique ☒ les États-Unis d'Amérique seulement ☐ les États indiqués dans le cadre supplémentaire

☒ D'autres déposants ou inventeurs sont indiqués sur une feuille annexe.

Cadre n° IV MANDATAIRE OU REPRÉSENTANT COMMUN; OU ADRESSE POUR LA CORRESPONDANCE

La personne dont l'identité est donnée ci-dessous est/a été désignée pour agir au nom du ou des déposants auprès des autorités internationales compétentes, comme: ☒ mandataire ☐ représentant commun

Nom et adresse : *(Nom de famille suivi du prénom; pour une personne morale, désignation officielle complète. L'adresse doit comprendre le code postal et le nom du pays.)*

COLOMBE Michel
BULL S.A.
68, route de Versailles (P.C. : 58D20)
78434 LOUVECIENNES Cedex
France

n° de téléphone: 33 (1) 39.66.61.71

n° de télécopieur: 33 (1) 39.66.61.73

n° de téléimprimeur:

☐ **Adresse pour la correspondance** : cocher cette case lorsque aucun mandataire ni représentant commun n'est/n'a été désigné et que l'espace ci-dessus est utilisé pour indiquer une adresse spéciale à laquelle la correspondance doit être envoyée.

PCT 754/301299

Suite du cadre n° III AUTRE(S) DÉPOSANT(S) OU (AUTRE(S)) INVENTEUR(S)

Si aucun des sous-cadres suivants n'est utilisé, cette feuille ne doit pas être incluse dans la requête.

Nom et adresse : *(Nom de famille suivi du prénom; pour une personne morale, désignation officielle complète. L'adresse doit comprendre le code postal et le nom du pays. Le pays de l'adresse indiquée dans ce cadre est l'État où le déposant a son domicile si aucun domicile n'est indiqué ci-dessous.)*

MARTIN René
32, rue Gometz
91440 BURES SUR YVETTE
FRANCE

Cette personne est :
- ☐ déposant seulement
- ☒ déposant et inventeur
- ☐ inventeur seulement *(Si cette case est cochée, ne pas remplir la suite.)*

Nationalité (nom de l'État) : FRANCE

Domicile (nom de l'État) : FRANCE

Cette personne est déposant pour : ☐ tous les États désignés ☐ tous les États désignés sauf les États-Unis d'Amérique ☒ les États-Unis d'Amérique seulement ☐ les États indiqués dans le cadre supplémentaire

Nom et adresse : *(Nom de famille suivi du prénom; pour une personne morale, désignation officielle complète. L'adresse doit comprendre le code postal et le nom du pays. Le pays de l'adresse indiquée dans ce cadre est l'État où le déposant a son domicile si aucun domicile n'est indiqué ci-dessous.)*

TRAN MINH Lap
18, rue Paul Eluard
95360 MONTMAGNY
FRANCE

Cette personne est :
- ☐ déposant seulement
- ☒ déposant et inventeur
- ☐ inventeur seulement *(Si cette case est cochée, ne pas remplir la suite.)*

Nationalité (nom de l'État) : FRANCE

Domicile (nom de l'État) : FRANCE

Cette personne est déposant pour : ☐ tous les États désignés ☐ tous les États désignés sauf les États-Unis d'Amérique ☒ les États-Unis d'Amérique seulement ☐ les États indiqués dans le cadre supplémentaire

Nom et adresse : *(Nom de famille suivi du prénom; pour une personne morale, désignation officielle complète. L'adresse doit comprendre le code postal et le nom du pays. Le pays de l'adresse indiquée dans ce cadre est l'État où le déposant a son domicile si aucun domicile n'est indiqué ci-dessous.)*

Cette personne est :
- ☐ déposant seulement
- ☐ déposant et inventeur
- ☐ inventeur seulement *(Si cette case est cochée, ne pas remplir la suite.)*

Nationalité (nom de l'État) :

Domicile (nom de l'État) :

Cette personne est déposant pour : ☐ tous les États désignés ☐ tous les États désignés sauf les États-Unis d'Amérique ☐ les États-Unis d'Amérique seulement ☐ les États indiqués dans le cadre supplémentaire

Nom et adresse : *(Nom de famille suivi du prénom; pour une personne morale, désignation officielle complète. L'adresse doit comprendre le code postal et le nom du pays. Le pays de l'adresse indiquée dans ce cadre est l'État où le déposant a son domicile si aucun domicile n'est indiqué ci-dessous.)*

Cette personne est :
- ☐ déposant seulement
- ☐ déposant et inventeur
- ☐ inventeur seulement *(Si cette case est cochée, ne pas remplir la suite.)*

Nationalité (nom de l'État) :

Domicile (nom de l'État) :

Cette personne est déposant pour : ☐ tous les États désignés ☐ tous les États désignés sauf les États-Unis d'Amérique ☐ les États-Unis d'Amérique seulement ☐ les États indiqués dans le cadre supplémentaire

☐ D'autres déposants ou inventeurs sont indiqués sur une autre feuille annexe.

Cadre n° V DÉSIGNATION D'ÉTATS

Les désignations suivantes sont faites conformément à la règle 4.9.a) *(cocher les cases appropriées; [illegible] au moins doit l'être)* :

Brevet régional

☐ **AP** **Brevet ARIPO : GH** Ghana, **GM** Gambie, **KE** Kenya, **LS** Lesotho, **MW** Malawi, **SD** Soudan, **SL** Sierra Leone, **SZ** Swaziland, **TZ** République-Unie de Tanzanie, **UG** Ouganda, **ZW** Zimbabwe et tout autre État qui est un État contractant du Protocole de Harare et du PCT

☐ **EA** **Brevet eurasien : AM** Arménie, **AZ** Azerbaïdjan, **BY** Bélarus, **KG** Kirghizistan, **KZ** Kazakhstan, **MD** République de Moldova, **RU** Fédération de Russie, **TJ** Tadjikistan, **TM** Turkménistan et tout autre État qui est un État contractant de la Convention sur le brevet eurasien et du PCT

☒ **EP** **Brevet européen : AT** Autriche, **BE** Belgique, **CH et LI** Suisse et Liechtenstein, **CY** Chypre, **DE** Allemagne, **DK** Danemark, **ES** Espagne, **FI** Finlande, **FR** France, **GB** Royaume-Uni, **GR** Grèce, **IE** Irlande, **IT** Italie, **LU** Luxembourg, **MC** Monaco, **NL** Pays-Bas, **PT** Portugal, **SE** Suède et tout autre État qui est un État contractant de la Convention sur le brevet européen et du PCT

☐ **OA** **Brevet OAPI : BF** Burkina Faso, **BJ** Bénin, **CF** République centrafricaine, **CG** Congo, **CI** Côte d'Ivoire, **CM** Cameroun, **GA** Gabon, **GN** Guinée, **GW** Guinée-Bissau, **ML** Mali, **MR** Mauritanie, **NE** Niger, **SN** Sénégal, **TD** Tchad, **TG** Togo et tout autre État qui est un État membre de l'OAPI et un État contractant du PCT *(si une autre forme de protection ou de traitement est souhaitée, le préciser sur la ligne pointillée)* . . . . . .

Brevet national *(si une autre forme de protection ou de traitement est souhaitée, le préciser sur la ligne pointillée)* :

☐ **AE** Émirats arabes unis
☐ **AL** Albanie . . . . . .
☐ **AM** Arménie . . . . . .
☐ **AT** Autriche . . . . . .
☐ **AU** Australie . . . . . .
☐ **AZ** Azerbaïdjan
☐ **BA** Bosnie-Herzégovine . . . . . .
☐ **BB** Barbade
☐ **BG** Bulgarie . . . . . .
☐ **BR** Brésil . . . . . .
☐ **BY** Bélarus . . . . . .
☐ **CA** Canada
☐ **CH et LI** Suisse et Liechtenstein
☐ **CN** Chine . . . . . .
☐ **CR** Costa Rica . . . . . .
☐ **CU** Cuba . . . . . .
☐ **CZ** République tchèque . . . . . .
☐ **DE** Allemagne . . . . . .
☐ **DK** Danemark . . . . . .
☐ **DM** Dominique
☐ **EE** Estonie . . . . . .
☐ **ES** Espagne . . . . . .
☐ **FI** Finlande . . . . . .
☐ **GB** Royaume-Uni
☐ **GD** Grenade
☐ **GE** Géorgie . . . . . .
☐ **GH** Ghana . . . . . .
☐ **GM** Gambie
☐ **HR** Croatie . . . . . .
☐ **HU** Hongrie . . . . . .
☐ **ID** Indonésie
☐ **IL** Israël . . . . . .
☐ **IN** Inde . . . . . .
☐ **IS** Islande
☐ **JP** Japon . . . . . .
☐ **KE** Kenya . . . . . .
☐ **KG** Kirghizistan . . . . . .
☐ **KP** République populaire démocratique de Corée . . . . . .
☐ **KR** République de Corée . . . . . .
☐ **KZ** Kazakhstan . . . . . .
☐ **LC** Sainte-Lucie
☐ **LK** Sri Lanka
☐ **LR** Liberia
☐ **LS** Lesotho . . . . . .
☐ **LT** Lituanie
☐ **LU** Luxembourg
☐ **LV** Lettonie
☐ **MA** Maroc . . . . . .
☐ **MD** République de Moldova . . . . . .
☐ **MG** Madagascar . . . . . .
☐ **MK** Ex-République yougoslave de Macédoine . . . . . .
☐ **MN** Mongolie
☐ **MW** Malawi . . . . . .
☐ **MX** Mexique . . . . . .
☐ **NO** Norvège
☐ **NZ** Nouvelle-Zélande . . . . . .
☐ **PL** Pologne . . . . . .
☐ **PT** Portugal . . . . . .
☐ **RO** Roumanie
☐ **RU** Fédération de Russie . . . . . .
☐ **SD** Soudan
☐ **SE** Suède
☐ **SG** Singapour
☐ **SI** Slovénie . . . . . .
☐ **SK** Slovaquie . . . . . .
☐ **SL** Sierra Leone . . . . . .
☐ **TJ** Tadjikistan . . . . . .
☐ **TM** Turkménistan . . . . . .
☐ **TR** Turquie . . . . . .
☐ **TT** Trinité-et-Tobago . . . . . .
☐ **TZ** République-Unie de Tanzanie
☐ **UA** Ukraine . . . . . .
☐ **UG** Ouganda . . . . . .
☒ **US** États-Unis d'Amérique . . . . . .
☐ **UZ** Ouzbékistan . . . . . .
☐ **VN** Viet Nam . . . . . .
☐ **YU** Yougoslavie . . . . . .
☐ **ZA** Afrique du Sud . . . . . .
☐ **ZW** Zimbabwe . . . . . .

Cases réservées pour la désignation d'États qui sont devenus parties au PCT après la publication de la présente feuille :

☐ . . . . . .
☐ . . . . . .

Déclaration concernant les désignations de précaution : outre les désignations faites ci-dessus, le déposant fait aussi conformément à la règle 4.9.b) toutes les désignations qui seraient autorisées en vertu du PCT, à l'exception de toute désignation indiquée dans le cadre supplémentaire comme étant exclue de la portée de cette déclaration. Le déposant déclare que ces désignations additionnelles sont faites sous réserve de confirmation et que toute désignation qui n'est pas confirmée avant l'expiration d'un délai de 15 mois à compter de la date de priorité doit être considérée comme retirée par le déposant à l'expiration de ce délai. *(La confirmation (y compris les taxes) doit parvenir à l'office récepteur dans le délai de 15 mois.)*

Cadre n° VI REVENDICATION DE PRIORITÉ

☐ D'autres revendications de priorité sont indiquées dans le cadre supplémentaire.

Date de dépôt de la demande antérieure *(jour/mois/année)*	Numéro de la demande antérieure	Lorsque la demande antérieure est une : demande nationale : pays	demande régionale :* office régional	demande internationale : office récepteur
(1) 23 novembre 1999 (23.11.99)	99 14755	FRANCE		
(2)				
(3)				

☒ L'office récepteur est prié de préparer et de transmettre au Bureau international une copie certifiée conforme de la ou des demandes antérieures *(seulement si la demande antérieure a été déposée auprès de l'office qui, aux fins de la présente demande internationale, est l'office récepteur)* indiquées ci-dessus au(x) point(s) : 1

** Si la demande antérieure est une demande ARIPO, il est obligatoire d'indiquer dans le cadre supplémentaire au moins un pays partie à la Convention de Paris pour la protection de la propriété industrielle pour lequel cette demande antérieure a été déposée (règle 4.10.b)ii)). Voir le cadre supplémentaire.*

Cadre n° VII ADMINISTRATION CHARGÉE DE LA RECHERCHE INTERNATIONALE

Choix de l'administration chargée de la recherche internationale (ISA) *(si plusieurs administrations chargées de la recherche internationale sont compétentes pour procéder à la recherche internationale, indiquer l'administration choisie; le code à deux lettres peut être utilisé) :*

ISA / FRANCE

Demande d'utilisation des résultats d'une recherche antérieure; mention de cette recherche *(si une recherche antérieure a été effectuée par l'administration chargée de la recherche internationale ou demandée à cette dernière) :*

Date *(jour/mois/année)* 04.10.2000 Numéro FA 583761 Pays *(ou office régional)* FRANCE

Cadre n° VIII BORDEREAU; LANGUE DE DÉPÔT

La présente demande internationale contient le **nombre de feuilles** suivant :

requête	4
description (sauf partie réservée au listage des séquences)	15
revendications	2
abrégé	1
dessins	9
partie de la description réservée au listage des séquences	
Nombre total de feuilles	31

Le ou les éléments cochés ci-après **sont joints à** la présente demande internationale :

1. ☐ feuille de calcul des taxes
2. ☐ pouvoir distinct signé
3. ☐ copie du pouvoir général; numéro de référence, le cas échéant :
4. ☐ explication de l'absence d'une signature
5. ☐ document(s) de priorité indiqué(s) dans le cadre n° VI au(x) point(s) :
6. ☐ traduction de la demande internationale en (langue) :
7. ☐ indications séparées concernant des micro-organismes ou autre matériel biologique déposés
8. ☐ listage des séquences de nucléotides ou d'acides aminés sous forme déchiffrable par ordinateur
9. ☐ autres éléments *(préciser)* :

Figure des dessins qui doit accompagner l'abrégé : 2

Langue de dépôt de la demande internationale : Français

Cadre n° IX SIGNATURE DU DÉPOSANT OU DU MANDATAIRE

À côté de chaque signature, indiquer le nom du signataire et, si cela n'apparaît pas clairement à la lecture de la requête, à quel titre l'intéressé signe.

Michel COLOMBE (Mandataire Bull S.A.)

Réservé à l'office récepteur

1. Date effective de réception des pièces supposées constituer la demande internationale :
2. Dessins : ☐ reçus : ☐ non reçus :
3. Date effective de réception, rectifiée en raison de la réception ultérieure, mais dans les délais, de documents ou de dessins complétant ce qui est supposé constituer la demande internationale :
4. Date de réception, dans les délais, des corrections demandées selon l'article 11.2) du PCT :
5. Administration chargée de la recherche internationale (si plusieurs sont compétentes) : ISA /
6. ☐ Transmission de la copie de recherche différée jusqu'au paiement de la taxe de recherche.

Réservé au Bureau international

Date de réception de l'exemplaire original par le Bureau international :

TRAITE DE COOPERATION EN MATIERE DE BREVETS

Expéditeur: le BUREAU INTERNATIONAL

PCT

NOTIFICATION DE LA RECEPTION DE L'EXEMPLAIRE ORIGINAL

(règle 24.2.a) du PCT)

Destinataire:

COLOMBE, Michel
Bull S.A.
68, route de Versailles
F-78434 Louveciennes Cedex
FRANCE

Renvoi

Date d'expédition (jour/mois/année)	NOTIFICATION IMPORTANTE
13 février 2001 (13.02.01)	
Référence du dossier du déposant ou du mandataire	**Demande internationale no**
PCT 3876 JMD	PCT/FR00/03230

Il est notifié au déposant que le Bureau international a reçu l'exemplaire original de la demande internationale précisée ci-après.

Nom(s) du ou des déposants et de l'Etat ou des Etats pour lesquels ils sont déposants:

BULL S.A. (pour tous les Etats désignés sauf US)
CUNCHON, François etc. (pour US seulement)

Date du dépôt international	:	21 novembre 2000 (21.11.00)
Date(s) de priorité revendiquée(s)	:	23 novembre 1999 (23.11.99)
Date de réception de l'exemplaire original par le Bureau international	:	29 janvier 2001 (29.01.01)
Liste des offices désignés	:	

EP :AT,BE,CH,CY,DE,DK,ES,FI,FR,GB,GR,IE,IT,LU,MC,NL,PT,SE,TR
National :US

ATTENTION

Le déposant doit soigneusement vérifier les indications figurant dans la présente notification. En cas de divergence entre ces indications et celles que contient la demande internationale, il doit aviser immédiatement le Bureau international.

En outre, l'attention du déposant est appelée sur les renseignements donnés dans l'annexe en ce qui concerne

- [X] les délais dans lesquels doit être abordée la phase nationale
- [X] la confirmation des désignations faites par mesure de précaution
- [ ] les exigences relatives aux documents de priorité.

Une copie de la présente notification est envoyée à l'office récepteur et à l'administration chargée de la recherche internationale.

Bureau international de l'OMPI
34, chemin des Colombettes
1211 Genève 20, Suisse

n° de télécopieur (41-22) 740.14.35

Fonctionnaire autorisé

Y. KUWAHARA

n° de téléphone (41-22) 338.83.38

ANNEXE DU FORMULAIRE PCT/IB/301

Demande internationale no PCT/FR00/03230

RENSEIGNEMENTS CONCERNANT LES DELAIS DANS LESQUELS DOIT ETRE ABORDEE LA PHASE NATIONALE

Il est rappelé au déposant qu'il doit aborder la "phase nationale" auprès de chacun des offices désignés indiqués sur la notification de la réception de l'exemplaire original (formulaire PCT/IB/301) en payant les taxes nationales et en remettant les traductions, telles qu'elles sont prescrites par les législations nationales.

Le délai d'accomplissement de ces actes de procédure est de **20 MOIS** à compter dela date de priorité ou, pour les Etats désignés qui ont été élus par le déposant dans une demande d'examen préliminaire international ou dans une élection ultérieure, de **30 MOIS** à compter de la date de priorité, à condition que cette électionait été effectuée avant l'expiration du 19e mois à compter de la date de priorité. Certains offices désignés (ou élus) ont fixé des délais qui expirent au-delà de 20 ou 30 mois à compter de la date de priorité. D'autres offices accordent une prolongation des délais ou un délai de grâce, dans certains cas moyennant le paiement d'une taxe supplémentaire.

En plus de ces actes de procédure, le déposant devra dans certains cas satisfaire à d'autres exigences particulières applicables dans certains offices. **Il appartient au déposant** de veiller à remplir en temps voulu les conditions requises pour l'ouverture de la phase nationale. La majorité des offices désignés n'envoient pas de rappel à l'approche de la date limite pour aborder la phase nationale.

Des informations détaillées concernant les actes de procédure à accomplir pour aborder la phase nationale auprès de chaque office désigné, les délais applicables et la possibilité d'obtenir une prolongation des délais ou un délai de grâce et toutes autres conditions applicables figurent dans le volume II du Guide du déposant du PCT. Les exigences concernant le dépôt d'une demande d'examen préliminaire international sont exposées dans le chapitre IX du volume I du Guide du déposant du PCT.

GR et ES sont devenues liées par le chapitre II du PCT le 7 septembre 1996 et le 8 septembre1997, respectivement, et peuvent donc être élues dans une demande d'examen préliminaire international ou dans une élection ultérieure présentée le 7 septembre 1996 (ou à une date postérieure) ou le 8 septembre 1997 (ou à une date postérieure), respectivement, quelle que soit la date de dépôt de la demande internationale (voir le second paragraphe, ci-dessus).

Veuillez noter que seul un déposant qui est ressortissant d'un Etat contractant du PCT lié par le chapitre II ou qui y a son domicile peut présenter une demande d'examen préliminaire international.

CONFIRMATION DES DESIGNATIONS FAITES PAR MESURE DE PRECAUTION

Seules les désignations expresses faites dans la requête conformément à la règle 4.9.a) figurent dans la présente notification. Il est important de vérifier si ces désignations ont été faites correctement. Des erreurs dans les désignations peuvent être corrigées lorsque des désignations ont été faites par mesure de précaution en vertu de la règle 4.9.b). Toute désignation ainsi faite peut être confirmée conformément aux dispositions de la règle 4.9.c) avant l'expiration d'un délai de 15 mois à compter de la date de priorité. En l'absence de confirmation, une désignation faite par mesure de précaution sera considérée comme retirée par le déposant. Il ne sera adressé aucun rappel ni invitation. Pour confirmer une désignation , il faut déposer une déclaration précisant l'Etat désigné concerné (avec l'indication de la forme de protection ou de traitement souhaitée) et payer les taxes de désignation et de confirmation. La confirmation doit parvenir à l'office récepteur dans le délai de 15 mois.

EXIGENCES RELATIVES AUX DOCUMENTS DE PRIORITE

Pour les déposants qui n'ont pas encore satisfait aux exigences relatives aux documents de priorité, il est rappelé ce qui suit.

Lorsque la priorité d'une demande nationale, régionale ou internationale antérieure est revendiquée, le déposant doit présenter une copie de cette demande antérieure, certifiée conforme par l'administration auprès de laquelle elle a été déposée ("document de priorité"), à l'office récepteur (qui la transmettra au Bureau international) ou directement au Bureau international, avant l'expiration d'un délai de 16 mois à compter de la date de priorité, étant entendu que tout document de priorité peut être présenté au Bureau international avant la date de publication de la demande internationale, auquel cas ce document sera réputé avoir été reçu par le Bureau international le dernier jour du délai de 16 mois (règle 17.1.a)).

Lorsque le document de priorité est délivré par l'office récepteur, le déposant peut, au lieu de présenter ce document, demander à l'office récepteur de le préparer et de le transmettre au Bureau international. La requête à cet effet doit être formulée avant l'expiration du délai de 16 mois et peut être soumise au paiement d'une taxe (règle 17.1.b)).

Si le document de priorité en question n'est pas fourni au Bureau international, ou si la demande adressée à l'office récepteur de préparer et de transmettre le document de priorité n'a pas été faite (et la taxe correspondante acquittée, le cas échéant) avant l'expiration du délai applicable mentionné aux paragraphes précédents, tout Etat désigné peut ne pas tenir compte de la revendication de priorité; toutefois, aucun office désigné ne peut décider de ne pas tenir compte de la revendication de priorité avant d'avoir donné au déposant la possibilité de remettre le document de priorité dans un délai raisonnable en l'espèce.

Lorsque plusieurs priorités sont revendiquées, la date de priorité à prendre en considération aux fins du calcul du délai de 16 mois est la date du dépôt de la demande la plus ancienne dont la priorité est revendiquée.

TRAITE DE COOPERATION EN MATIERE DE BREVETS

Expéditeur : le BUREAU INTERNATIONAL

PCT

NOTIFICATION RELATIVE A LA PRESENTATION OU A LA TRANSMISSION DU DOCUMENT DE PRIORITE

(instruction administrative 411 du PCT)

Rectificatif

Destinataire:

COLOMBE, Michel
Bull S.A.
68, route de Versailles
F-78434 Louveciennes Cedex
FRANCE

Date d'expédition (jour/mois/année) 13 février 2001 (13.02.01)	
Référence du dossier du déposant ou du mandataire PCT 3876 JMD	**NOTIFICATION IMPORTANTE**
Demande internationale no PCT/FR00/03230	Date du dépôt international (jour/mois/année) 21 novembre 2000 (21.11.00)
Date de publication internationale (jour/mois/année) 31 mai 2001 (31.05.01)	Date de priorité (jour/mois/année) 23 novembre 1999 (23.11.99)
Déposant BULL S.A. etc	

1. La date de réception (sauf lorsque les lettres "NR" figurent dans la colonne de droite) par le Bureau international du ou des documents de priorité correspondant à la ou aux demandes énumérées ci-après est notifiée au déposant. Sauf indication contraire consistant en un astérisque figurant à côté d'une date de réception, ou les lettres "NR", dans la colonne de droite, le document de priorité en question a été présenté ou transmis au Bureau international d'une manière conforme à la règle 17.1.a) ou b).
2. Ce formulaire met à jour et remplace toute notification relative à la présentation ou à la transmission du document de priorité qui a été envoyée précédemment.
3. Un **astérisque(*)** figurant à côté d'une date de réception dans la colonne de droite signale un document de priorité présenté ou transmis au Bureau international mais de manière non conforme à la règle 17.1.a) ou b). Dans ce cas, **l'attention du déposant est appelée** sur la règle 17.1.c) qui stipule qu'aucun office désigné ne peut décider de ne pas tenir compte de la revendication de priorité avant d'avoir donné au déposant la possibilité de remettre le document de priorité dans un délai raisonnable en l'espèce.
4. Les **lettres "NR"** figurant dans la colonne de droite signalent un document de priorité que le Bureau international n'a pas reçu ou que le déposant n'a pas demandé à l'office récepteur de préparer et de transmettre au Bureau international, conformément à la règle 17.1.a) ou b), respectivement. Dans ce cas, **l'attention du déposant est appelée** sur la règle 17.1.c) qui stipule qu'aucun office désigné ne peut décider de ne pas tenir compte de la revendication de priorité avant d'avoir donné au déposant la possibilité de remettre le document de priorité dans un délai raisonnable en l'espèce.

Date de priorité	Demande de priorité n°	Pays, office régional ou office récepteur selon le PCT	Date de réception du document de priorité
23 nove 1999 (23.11.99)	99/14755	FR	29 janv 2001 (29.01.01)

Bureau international de l'OMPI
34, chemin des Colombettes
1211 Genève 20, Suisse

no de télécopieur (41-22) 740.14.35

Fonctionnaire autorisé:

Y. KUWAHARA

no de téléphone (41-22) 338.83.38

TRAITE DE COOPERATION EN MATIERE DE BREVETS

Expéditeur: le BUREAU INTERNATIONAL

PCT

AVIS INFORMANT LE DEPOSANT DE LA COMMUNICATION DE LA DEMANDE INTERNATIONALE AUX OFFICES DESIGNES

(règle 47.1.c), première phrase, du PCT)

Destinataire:
COLOMBE, Michel
Bull S.A.
68, route de Versailles
F-78434 Louveciennes Cedex
FRANCE

Direction de la Propriété Intell...
12 JUIN 2001
BULL S.A.

Date d'expédition (jour/mois/année) 31 mai 2001 (31.05.01)	
Référence du dossier du déposant ou du mandataire PCT 3876 JMD	**AVIS IMPORTANT**

Demande internationale no	**Date du dépôt international** (jour/mois/année)	**Date de priorité** (jour/mois/année)
PCT/FR00/03230	21 novembre 2000 (21.11.00)	23 novembre 1999 (23.11.99)

Déposant
BULL S.A. etc

1. Il est notifié par la présente qu'à la date indiquée ci-dessus comme date d'expédition de cet avis, le Bureau international a communiqué, comme le prévoit l'article 20, la demande internationale aux offices désignés suivants:
   US

   Conformément à la règle 47.1.c), troisième phrase, ces offices acceptent le présent avis comme preuve déterminante du fait que la communication de la demande internationale a bien eu lieu à la date d'expédition indiquée plus haut, et le déposant n'est pas tenu de remettre de copie de la demande internationale à l'office ou aux offices désignés.

2. Les offices désignés suivants ont renoncé à l'exigence selon laquelle cette communication doit être effectuée à cette date:
   EP

   La communication sera effectuée seulement sur demande de ces offices. De plus, le déposant n'est pas tenu de remettre de copie de la demande internationale aux offices en question (règle 49.1)a-bis)).

3. Le présent avis est accompagné d'une copie de la demande internationale publiée par le Bureau international le
   31 mai 2001 (31.05.01) sous le numéro WO 01/39466

RAPPEL CONCERNANT LE CHAPITRE II (article 31.2)a) et règle 54.2)

Si le déposant souhaite reporter l'ouverture de la phase nationale jusqu'à 30 mois (ou plus pour ce qui concerne certains offices) à compter de la date de priorité, **la demande d'examen préliminaire international** doit être présentée à l'administration compétente chargée de l'examen préliminaire international avant l'expiration d'un délai de 19 mois à compter de la date de priorité.

Il appartient exclusivement au déposant de veiller au respect du délai de 19 mois.

Il est à noter que seul un déposant qui est ressortissant d'un Etat contractant du PCT lié par le chapitre II ou qui y a son domicile peut présenter une demande d'examen préliminaire international.

RAPPEL CONCERNANT L'OUVERTURE DE LA PHASE NATIONALE (article 22 ou 39.1))

Si le déposant souhaite que la demande internationale procède en phase nationale, il doit, dans le délai de 20 mois ou de 30 mois, ou plus pour ce qui concerne certains offices, accomplir les actes mentionnés dans ces dispositions auprès de chaque office désigné ou élu.

Pour d'autres informations importantes concernant les délais et les actes à accomplir pour l'ouverture de la phase nationale, voir l'annexe du formulaire PCT/IB/301 (Notification de la réception de l'exemplaire original) et le volume II du Guide du déposant du PCT.

Bureau international de l'OMPI
34, chemin des Colombettes
1211 Genève 20, Suisse

no de télécopieur (41-22) 740.14.35

Fonctionnaire autorisé
J. Zahra

no de téléphone (41-22) 338.83.38

Suite du formulaire PCT/IB/308

AVIS INFORMANT LE DEPOSANT DE LA COMMUNICATION DE LA DEMANDE INTERNATIONALE AUX OFFICES DESIGNES

Date d'expédition (jour/mois/année) 31 mai 2001 (31.05.01)	**AVIS IMPORTANT**
Référence du dossier du déposant ou du mandataire PCT 3876 JMD	**Demande internationale no** PCT/FR00/03230

Il est notifié au déposant que, au moment de l'établissement du présent avis, le délai fixé à la règle 46.1 pour le dépôt de modifications selon l'article 19 n'était pas encore expiré et que le Bureau international n'avait pas reçu de modications ni de déclaration l'informant que le déposant ne souhaitait pas présenter de modifications.

TRAITE DE COOPERATION EN MATIERE DE BREVETS

PCT

RAPPORT DE RECHERCHE INTERNATIONALE

(article 18 et règles 43 et 44 du PCT)

Référence du dossier du déposant ou du mandataire PCT 3876 JMD	**POUR SUITE A DONNER** voir la notification de transmission du rapport de recherche internationale (formulaire PCT/ISA/220) et, le cas échéant, le point 5 ci-après	
Demande internationale n° PCT/FR 00/ 03230	Date du dépôt international *(jour/mois/année)* 21/11/2000	(Date de priorité (la plus ancienne) *(jour/mois/année)* 23/11/1999
Déposant BULL S.A		

Le présent rapport de recherche internationale, établi par l'administration chargée de la recherche internationale, est transmis au déposant conformément à l'article 18. Une copie en est transmise au Bureau international.

Ce rapport de recherche internationale comprend 3 feuilles.

[X] Il est aussi accompagné d'une copie de chaque document relatif à l'état de la technique qui y est cité.

1. **Base du rapport**

a. En ce qui concerne la **langue,** la recherche internationale a été effectuée sur la base de la demande internationale dans la langue dans laquelle elle a été déposée, sauf indication contraire donnée sous le même point.

[ ] la recherche internationale a été effectuée sur la base d'une traduction de la demande internationale remise à l'administration.

b. En ce qui concerne **les séquences de nucléotides ou d'acides aminés** divulguées dans la demande internationale (le cas échéant), la recherche internationale a été effectuée sur la base du listage des séquences :

[ ] contenu dans la demande internationale, sous forme écrite.

[ ] déposée avec la demande internationale, sous forme déchiffrable par ordinateur.

[ ] remis ultérieurement à l'administration, sous forme écrite.

[ ] remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur.

[ ] La déclaration, selon laquelle le listage des séquences présenté par écrit et fourni ultérieurement ne vas pas au-delà de la divulgation faite dans la demande telle que déposée, a été fournie.

[ ] La déclaration, selon laquelle les informations enregistrées sous forme déchiffrable par ordinateur sont identiques à celles du listage des séquences présenté par écrit, a été fournie.

2. [ ] **Il a été estimé que certaines revendications ne pouvaient pas faire l'objet d'une recherche** (voir le cadre I).

3. [ ] **Il y a absence d'unité de l'invention** (voir le cadre II).

4. En ce qui concerne le **titre,**

[X] le texte est approuvé tel qu'il a été remis par le déposant.

[ ] Le texte a été établi par l'administration et a la teneur suivante:

5. En ce qui concerne **l'abrégé,**

[X] le texte est approuvé tel qu'il a été remis par le déposant

[ ] le texte (reproduit dans le cadre III) a été établi par l'administration conformément à la règle 38.2b). Le déposant peut présenter des observations à l'administration dans un délai d'un mois à compter de la date d'expédition du présent rapport de recherche internationale.

6. La figure **des dessins** à publier avec l'abrégé est la Figure n° 2

[X] suggérée par le déposant.

[ ] parce que le déposant n'a pas suggéré de figure.

[ ] parce que cette figure caractérise mieux l'invention.

[ ] Aucune des figures n'est à publier.

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/FR 00/03230

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 H04L29/06 G06F9/46

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 H04L G06F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
EPO-Internal, WPI Data, PAJ, INSPEC, IBM-TDB, COMPENDEX

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	US 5 485 579 A (LAU JAMES ET AL) 16 janvier 1996 (1996-01-16) colonne 12, ligne 62 -colonne 14, ligne 39 colonne 19, ligne 32 -colonne 20, ligne 7 colonne 21, ligne 31-44 colonne 26, ligne 11-41 ---	1-5
A	EP 0 942 369 A (LUCENT TECHNOLOGIES INC) 15 septembre 1999 (1999-09-15) colonne 4, ligne 20-41 colonne 7, ligne 55 -colonne 10, ligne 5 --- -/--	1-5

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
30 mars 2001	06/04/2001

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Lázaro, M.L.

1

Formulaire PCT/ISA/210 (deuxième feuille) (juillet 1992)

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec,le cas échéant, l'indicationdes passages pertinents	no. des revendications visées
A	HUNT R: "Internet/Intranet firewall security-policy, architecture and transaction services" COMPUTER COMMUNICATIONS,GB,BUTTERWORTHS & CO. PUBLISHERS LTD, vol. 21, no. 13, 1 septembre 1998 (1998-09-01), pages 1107-1123, XP004146571 ISSN: 0140-3664 page 1117, ligne 31 -page 1118, ligne 10 page 1120, ligne 38 -page 1121, ligne 14 figure 11 ---	1-5
A	LIU Y ET AL: "OSI remote procedure call: Standardization issues, design and implementation" COMPUTER COMMUNICATIONS,NL,ELSEVIER SCIENCE PUBLISHERS BV, AMSTERDAM, vol. 20, no. 6, 25 juillet 1997 (1997-07-25), pages 462-474, XP004126700 ISSN: 0140-3664 page 466, ligne 18 -page 468, ligne 37 -----	1-5

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inter[redacted]l Application No
PCT/[redacted]R 00/03230

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5485579 A	16-01-1996	US 6065037 A	16-05-2000
		AT 179811 T	15-05-1999
		AU 651321 B	21-07-1994
		AU 6436190 A	18-04-1991
		CA 2066566 A	09-03-1991
		DE 69033092 D	10-06-1999
		EP 0490980 A	24-06-1992
		IL 95449 A	07-10-1994
		JP 2945757 B	06-09-1999
		JP 5502127 T	15-04-1993
		KR 201772 B	15-06-1999
		WO 9104540 A	04-04-1991
EP 0942369 A	15-09-1999	CN 1233016 A	27-10-1999
		JP 11296389 A	29-10-1999